MaaS360®
by Fiberlink, an IBM company

IBM MaaS360 Mobile Device Management (MDM)

Installation Guide

Version 2, Release 2

Fiberlink Communications Corporation
1787 Sentry Parkway West
Blue Bell, PA 19422

February 2015

Table of Contents

Introduction

IBM® MaaS360 requires a series of distinct installation steps to fully deploy.

Read this document to find the information you need before you begin installation, to guide you through the installation and to configure your new deployment.

The first step is to understand the IBM MaaS360 deployment architecture. This document explains the various components of the deployment as well as how they interact with each other.

Hardware and software requirements are fully described, including the requirements for your VMware environment and your Oracle database server. Various software tools, several types of certificates and specific network configurations are required. You should review this information, procure the necessary components, and set up your infrastructure before beginning the installation.

After your installation environment is prepared and the necessary tools are gathered, the process of installation and configuration of your new deployment is described.

Below is a brief outline of the major sections of this document:

- Deployment architecture
- Hardware requirements
- Software, certificate, and network requirements
- High Availability guidelines
- Backup guidelines
- Deployment checklist
- Oracle Database deployment
- IBM MaaS360 installation
- IBM MaaS360 Administration Console configuration

Supported Devices and Infrastructure

IBM MaaS360 supports most mobile devices and infrastructures.

Devices can be managed by an agent installed on the device or through platform-specific management tools, such as BlackBerry Enterprise Server, Exchange Server, and so on.

Agent-Based Device Support

Devices can be managed by agents installed directly on the managed device.

The following OS versions support agent management:

- iOS 5.x, 6.x, 7.x, 8.x
- Android 2.2+ for IBM MaaS360 MDM
- Android 4.0+ for IBM MaaS360 Secure Productivity Suite (SPS)
- Windows Phone 8.0, 8.1

Platform-Based Device Support

Devices can be managed through platform management tools using the IBM MaaS360 Cloud Extender. For more information, see the IBM MaaS360 Cloud Extender Guide.

The IBM MaaS360 Cloud Extender supports the following platform versions:

- Microsoft Exchange Server 2007, 2010, 2013
- Microsoft Office 365
- BlackBerry Enterprise Server 5.0+
- IBM Lotus® Domino® 8.5.2
- IBM Notes® Traveler 8.5.2

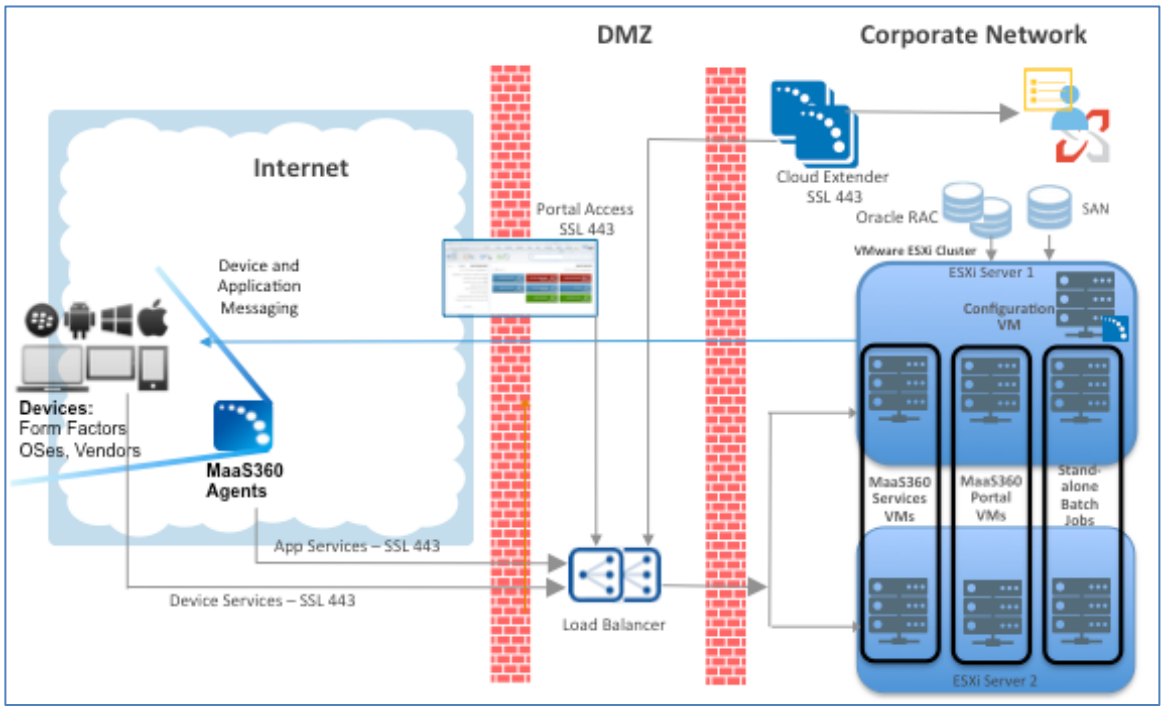
Deployment Architecture

IBM MaaS360 On-Premises is deployed as a set of virtual machines within a Virtual Appliance format (vApp) on the VMware ESXi Servers. These virtual machines interact with various other components that are hosted in the network to deliver a complete mobile device management solution.

The virtual appliance can be deployed in the DMZ or inside the internal network (as shown below) by configuring a reverse proxy or load balancer in the DMZ to interact with the virtual appliance.

It works in conjunction with various other components that are hosted in your network, to deliver a complete mobile device management solution. For IBM MaaS360 to communicate effectively with mobile devices, certain components must be visible on the public Internet.

The following diagram outlines the interaction between the components:



Virtual Machines

The IBM MaaS360 vApp includes seven virtual machines. Internal hostnames for the can be found in Appendix A: VM Internal Hostnames and IP Requirements.

Configuration VM

This virtual machine is used for deployment and administration of IBM MaaS360. It also hosts the IBM MaaS360 Administration Console (MAC), a web-based utility for configuring and deploying IBM MaaS360. This will be referred to as the *Configuration VM* in this document. There is one Configuration VM.

Portal VM

This includes the IBM MaaS360 Portal—a console that allows administrators to manage end users' devices; End User Portal—an application to allow end users to manage their own devices; Device

Enrollment—a workflow allowing end users to enroll new devices. This will be referred to as the *Portal VM* in the documentation. There are two Portal VMs.

Standalone Batch Jobs VM

This virtual machine runs the different scheduled batch jobs for IBM MaaS360. This will be referred to as the *Standalone VM* in the documentation. There are two Standalone Batch Jobs VMs.

Services and CDN (Content Delivery Network) VM

This virtual machine acts as a gateway for all end user device communications and API calls. It also hosts the content repository for distributing applications and documents to different end user devices. There are two Services and CDN VMs.

When any document or application is uploaded through the IBM MaaS360 Portal, the content gets uploaded onto the content repository. Devices are notified to pull the content from a specified services tier. This VM is referred to as the Services VM.

Databases

IBM MaaS360 creates four databases on your Oracle database server.

VPN2

This is the real-time transactional database that hosts device data and data for most portal workflows.

AGILINK

This database is the primary point of entry for new account information.

EDW

This is a vast data warehouse for supporting reports. Data from the VPN2 database is periodically loaded into the EDW.

P03

This database is used for log processing.

IBM MaaS360 Cloud Extender

The IBM MaaS360 Cloud Extender connects IBM MaaS360 to various enterprise systems such as Active Directory servers, SCEP servers, BES servers, Exchange ActiveSync, and Lotus Traveler servers within your environment. It is a Windows application that is installed on a separate Windows computer or VM. This application must be downloaded and installed after the IBM MaaS360 virtual appliance deployment is complete.

IBM MaaS360 Mobile Enterprise Gateway

The IBM MaaS360 Mobile Enterprise Gateway is an optional component that allows organizations to provide secure access to behind-the-firewall resources such as SharePoint, Windows File Share content, and Intranet sites on Mobile devices without a VPN connection. It is installed on a separate Windows computer or VM within the DMZ.

Hardware Requirements

A number of hardware components are required based on your anticipated device enrollment and deployment architecture.

The primary hardware components are a VMware ESXi Server where a vApp is deployed, and an Oracle Database Server.

VMware and Oracle Servers

There are recommended specifications for a non-native high availability deployment, based on the number of managed devices.

Important

For high availability deployment the specifications mentioned below have to be doubled.

The following table describes the recommended specifications.

Table 1. Recommended Specifications

	Oracle Database Server			ESXi Server		
Managed Devices	**Storage in GB**	**Memory in GB**	**CPU Cores**	**Storage in GB**	**Memory in GB**	**CPU Cores**
2000	150	8	1	400	40	6
5000	150	8	2	400	40	8
10000	200	16	4	400	40	8
25000	200	24	4	400	48	8
50000	350	48	8	500	56	10
100000	500	96	8	700	64	12
200000	700	144	10	1000	80	16
400000	1000	256	12	1500	112	16
500000	1000	304	12	1500	128	20

Note: *The storage space that is specified for the database server is required for IBM MaaS360 data only. Extra storage must be available for Oracle and backup data.*

SMTP Server

An SMTP email server is required to facilitate email communication to administrators and users.

Ensure that the SMTP email server is within your firewall and that the port selected during installation is open. The default port is typically port 25.

Network File System (NFS) Server

MaaS360 supports integration with an external NFS server for Content Data Network (CDN) storage. This is a mandatory requirement for native high availability deployment.

The NFS server should be configured as follows:

1. Default NFS version should be 3

   `File - /etc/nfsmount.conf [ Defaultvers=3 ]`

2. Export Directory/Path should have ownership as follows

   UID : 1011

   GID : 1026

   e.g., `drwxrwxr-x 8 1011 1026 4096 Dec  2 23:58 /export/directory/path/`

3. In `/etc/exports` file, permissions should be (rw,sync,no_root_squash) for the IP addresses of Services and Standalone VMs.

   e.g, `/export/directory/path/ xx.xx.xx.xx(rw,sync,no_root_squash)`

Note: *For high availability deployment, make sure you add IP addresses of the two Services VMs and two Standalone VMs.*

4. IPtables/Firewall changes should be done to have Services and Standalone VMs access the NFS server at the configured port.

Note: *For high availability deployment, make sure you allow access to NFS server and port for the two Services VMs and two Standalone VMs.*

5. Reserve minimum of 100 GB in the NFS server for each customer account created in MaaS360.

   Based on actual utilization, this size is likely to vary.

Important

If the NFS server is not accessible from MaaS360 for some reason, uploading and downloading applications and documents is likely to fail. After connection is reestablished please allow up to 20 minutes for applications and documents upload/download to work properly.

Load Balancer

MaaS360 supports integration with an external load balancer server for native high availability deployment. This is a mandatory requirement for native high availability deployment.

Refer to the *MaaS360 High Availability Overview* document for more details.

Reverse Proxy

MaaS360 supports integration with an external reverse proxy server for reverse proxy deployment. This is a mandatory requirement for reverse proxy deployment.

Refer to the *MaaS360 High Availability Overview* document for more details.

Cloud Extender Requirements

The IBM MaaS360 Cloud Extender is an optional component in your deployment architecture. For more information about the IBM MaaS360 Cloud Extender, see the *IBM MaaS360 Cloud Extender Guide*.

Cloud Extender requirements vary based on the size of your deployment. The minimum specifications for the Cloud Extender are:

- Physical or virtual machine
- Windows Server 2008, 2008 R2, or 2012
- Pentium III, 500 MHz
- 1 GB RAM
- 2 GB Storage

Mobile Enterprise Gateway Requirements

The IBM MaaS360 Mobile Enterprise Gateway is an optional component in your deployment architecture. For more information about the IBM MaaS360 Mobile Enterprise Gateway, see the IBM MaaS360 Mobile Enterprise Gateway Administration Guide.

Mobile Enterprise Gateway requirements vary based on the size of your deployment. The minimum specifications for the Mobile Enterprise Gateway are:

- Physical or virtual machine
- Windows Server 2008, 2008 R2, or 2012
- Dual core CPU
- 2 GB RAM
- 1 GB Storage

Software and Network Requirements

IBM MaaS360 requires a series of software components including software licenses, certificates, and network settings. You are advised to obtain or configure these elements before installation.

Software Licenses and Downloads

The following software licenses and components are required for installation.

- Oracle Standard Edition One, Oracle Standard Edition or Oracle Enterprise Edition version 11.2.0.4.0 (64-bit).
- An Oracle supported OS for the database server.
- VMware software for your ESXi Server:
  - ESXi 5.x
  - vCenter Server 5.x
  - vSphere Client 5.x
  - Distributed Resource Scheduler (DRS)
- VMware vSphere Client to connect to your ESXi deployment from a Windows computer.
- Remote Connection Tools to connect to hosts and the Oracle database.
- IBM MaaS360 Virtual Application package (.ova).
- IBM MaaS360 Database Artifact package for Oracle 11.2.0.4.0
- Oracle Database Configuration Assistant (DBCA).
- Chrome, Firefox, or Internet Explorer Browser. IE 11+ is the only currently supported version.
- Optional: iOS Enterprise Developer Program account. This is necessary for managing iOS devices.
- Optional: Google Cloud Messaging (GCM) API key. This is necessary for managing Android devices.
- Optional: Microsoft Bing Maps key allows device tracking features.
- Optional: SMS Gateway account from either Tropo or Clickatell.
- Optional: Veracode account for Application Reputation ratings.

Certificate Requirements

Several certificates are required for secure communication between infrastructure components. To ensure a quick installation process, you are recommended to acquire these certificates before beginning installation.

Table 2. Certificates

Certificate	Description
iOS Code Signing Certificate	To enroll iOS devices, the IBM MaaS360 for iOS agent must be signed by your iOS Code Signing Certificate. This certificate is required only if you plan to manage iOS devices. For more information about the iOS Enterprise Developer Program, and obtaining an iOS Code Signing Certificate, see https://developer.apple.com/programs/ios/.
Symantec Windows Phone Code Signing Certificate	To enroll Windows Phone 8+ devices, the IBM MaaS360 for Windows Phone agent must be signed by your Windows Phone Code Signing certificate. For more information, see the *IBM MaaS360® Mobile Device Management Configuration Guide*. This certificate is required to manage Windows Phone devices only.
Apple Push Notification Service (APNS)	To manage iOS devices, an APNS certificate from Apple is required. This certificate is not required during installation. For more information on obtaining an APNS certificate, see the *IBM MaaS360 Mobile Device Management Configuration Guide*.
SSL Certificates	One or more SSL certificates, signed by a trusted certificate authority (CA), are required for MaaS360 DNS URLs. If you are using an external load balancer or reverse proxy then ensure you use only trusted SSL certificates for them. SSL certificate private keys are normally protected by a password. This password must be removed from the private key. For more information, see Appendix D: SSL Certificate Password Removal.

Network Configuration

Check your network configuration before beginning the installation to make sure that the following requirements are met:

Table 3. Network Requirements

Item	Description
Internal IP Addresses	The IBM MaaS360 vApp requires seven internal IP addresses from the same subnet for the virtual machines. It also requires IP addresses for the DNS servers, subnet mask and default gateway. For more information, see Appendix A: VM Internal Hostnames and IP Requirements.

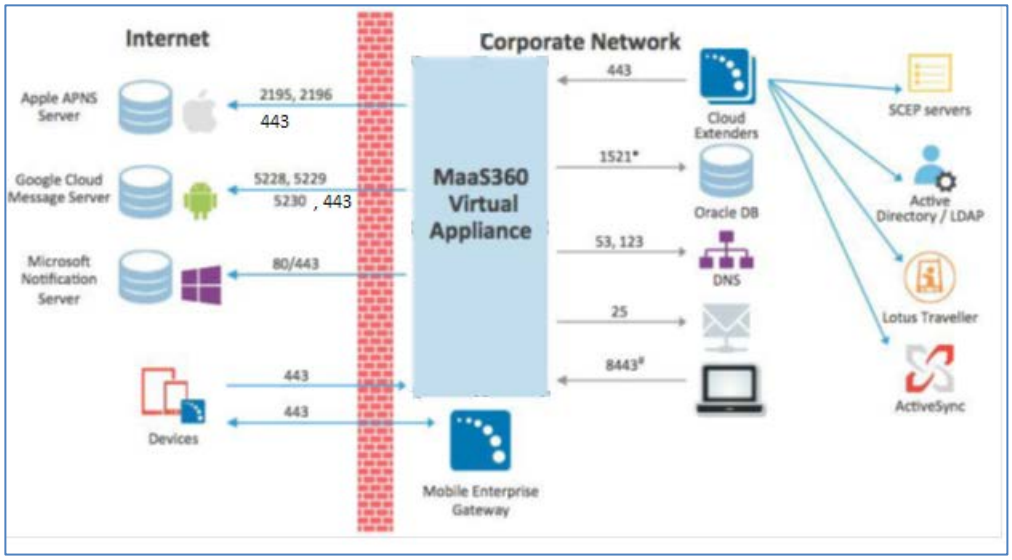
Item	Description
External IP Addresses	Minimum of one external IP address and up to four external IP addresses at the external load balancer for native high availability deployment. Minimum of one external IP address and up to two external IP addresses at the external reverse proxy for reverse proxy deployment. For non-native high availability deployment, a set of two external IP addresses for the Portal VM and the Services VMs. One external IP can be used for the Portal, End User Portal and Enrollment DNS. The Services DNS requires a dedicated external IP.
DNS Entries	Make the following DNS entries for virtual hosts and map them to the IP addresses reserved for respective URLs: • Device Services • End User Portal • Enrollments • Admin Portal • Gateway Service—required if you use IBM MaaS360 Mobile Enterprise Gateway • Administration Console—you can configure a FQDN for IBM MaaS360 Administration Console on internal DNS server to avoid accessing the console via IP address. It is recommended that the DNS entries be in the same domain. This allows a single wildcard SSL cert to be used. For example DNA entries, see Appendix B: Sample DNS Entries. Based on native high availability, reverse proxy or non-native high availability deployment, the DNS entries should be made suitably.
Network Ports	Make sure all network ports are configured on your external and internal firewall. For more information, see Firewall Ports.
Firewall	Content filter firewall rules for media content must be enabled for accessing the Apple VPP URL at https://vpp.itunes.apple.com/WebObjects/MZFinance.woa/wa/VPPServiceConfigSrv. The firewall must not be configured with a timeout.

Firewall Ports

Some ports must be opened on your firewalls to allow IBM MaaS360 to communicate with necessary resources.

The following diagram illustrates all the ports that must be opened on your firewalls to allow IBM MaaS360 to communicate with necessary resources.

Note: *1521 is the standard port for Oracle installation; replace 1521 with the appropriate port for your environment, if necessary. Port 8443 is required for the Administrator Console IP only.*



Note: *Your internal firewall should not be configured with a timeout between the VMs and the database.*

High Availability / Reverse Proxy Requirements

Some applications in MaaS360 VMs send requests to each other by using the external DNS URLs.

If MaaS360 is integrated with an external load balancer or reverse proxy server, then MaaS360 VMs need to be able to route requests to applications through the load balancer or reverse proxy. Ensure the VMs can send outgoing requests to the load balancer or reverse proxy at port 443. MaaS360 vApp should have access to the DNS Gateway needed for looking up the external DNS URL entries.

High Availability

IBM MaaS360 has the ability to configure the instance for native Active/Active High Availability. This configuration option offers customers the ability to deploy IBM MaaS360 to support environments where critical Enterprise Mobility Management services must be available at all times.

IBM MaaS360 Active/Active High Availability (HA) is achieved by leveraging inherent resilience within the architecture of MaaS360. MaaS360 can support Application, Database and Server/OS resilience. Application resilience is achieved by deploying two Portal VMs, two Services VMs and two Standalone VMs and utilizing a load balancer to direct traffic to the running VMs or to a single VM in the case of a failure. Hardware resilience is achieved by deploying the MaaS360 Virtual Machines across ESXi Servers in an ESXi cluster running on disparate hardware. Database resilience is achieved by deploying Oracle across at least two nodes using Real Application Clusters (RAC).

Please refer to the *MaaS360 High Availability Overview* **document** for more details.

Notes:

- *In case of non-native High Availability deployment (with four VMs), VMware High Availability (HA) and VMware Distributed Resource Scheduler (DRS) products can be utilized to provide Active/Passive high availability for MaaS30.*
- *In addition to software license requirements, the backbone of your HA deployment is one or more ESXi servers. Each server must meet the hardware requirements described in* Hardware Requirements.
- *Multiple ESXi servers must have a shared storage solution (SAN or NFS) that is part of the HA cluster. The IBM MaaS360 vApp must be deployed on this shared storage.*
- *The IBM MaaS360 High-Availability configuration will require familiarity with the standalone installation process and the various aspects of a successful installation including IP addressing, DNS, certificates, URLs and sizing of the instance. This information can be found in the* IBM MaaS360 Installation Guide *and the* IBM MaaS360 Configuration Guide.

Backup and Restore

A robust backup and recovery mechanism for IBM MaaS360 is essential to recover from catastrophic failures and eliminate data loss. A complete backup policy should include full backup capabilities as well as incremental backups.

This content is provided as a guideline. You are expected to define your own Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for IBM MaaS360 based on your requirements for uptime and data loss prevention.

Because the underlying technology used in IBM MaaS360 is VMware and Oracle, we recommend using the backup and recovery tools provided by these vendors. This is at your discretion; any tools you are comfortable with, or that meet your needs, are acceptable.

The components that should be part of your backup plan include:

- Virtual Appliance (vApp) and VMs
- Oracle databases: AGILINK, EDW, VPN2, and PO3
- Content Delivery Network (CDN), NFS export directory
- IBM MaaS360 Cloud Extender
- IBM MaaS360 Mobile Enterprise Gateway

Backup Frequency

Determine a backup schedule that is appropriate to your deployment.

The following backup schedule is recommended. This schedule can be altered to fit your RPO and RTO requirements.

Table 4. Recommended backup frequency

Component	Full backup	Incremental backup
vApp and VMs	Weekly	Daily
Oracle Database	Weekly	Daily
Cloud Extender	Weekly	Daily
Mobile Enterprise Gateway	Weekly	Daily
CDN Content backup, NFS export directory	Weekly	Daily

For a High Availability deployment, the CDN content will lie in the NFS server. The export directory in the NFS server that hosts CDN content for IBM MaaS360 has to be backed up and restored in case of failures.

For non-High Availability deployment, the CDN is part of the Services VM and is therefore backed up when the Services VM is backed up. However, it is possible to back up the content in the CDN independently, if desired, using a script. For more information, see CDN Backup.

The IBM MaaS360 Cloud Extender and IBM MaaS360 Mobile Enterprise Gateway are optional components that might not be part of your deployment.

Virtual Appliance Backup

When you back up the IBM MaaS360 VApp, be sure to include the backup and recovery of all aspects of the vApp environment.

Your chosen backup and recovery tools should have the capability to back up the entirety of the virtual appliance or every individual virtual machine. These include the Configuration, Portal, Standalone Batch Jobs, and Services & CDN virtual machines. The backup should capture both disk and memory data. In addition, your backup solution should allow full and incremental backups. Fast recovery by applying delta changes should also be supported. The ability to selectively restore individual files and folders within a virtual machine is also an advantage.

VMware vSphere Data Protection is the recommended tool to back up and restore your VWware environment. This tool meets all of the requirements listed. However, the choice of tool should be left to your VMware administrator based on the needs of your environment.

Oracle Database Backup

A full backup solution includes backup of your Oracle database environment, including all four databases that are part of your IBM MaaS360 deployment.

Your Oracle database backup solution should allow full and incremental backups of the four databases: AGELINK, EDW, VPN2, and PO3. The backup should include data files, control files, and archived redo logs.

The recommended backup tool for your Oracle environment is Oracle's Recovery Manager or RMAN. RMAN is fully integrated with Oracle database and it supports full backup, incremental backup using change tracking, binary compression, encryption, and cross platform data conversion.

Archive Log Mode should be enabled for the four Oracle databases for RMAN to function properly. Be sure to enable Archive Log Mode during database installation. For more information see Database Installation.

In addition, setting up a Flash Recovery Area, or FRA, is recommended. Using a FRA simplifies database backup by automatically naming recovery files, retaining them as long as they are needed for restore and recovery activities, and deleting them when they are no longer needed. The FRA should be sized according to your RPO and RTO policies.

Note: *Incremental backup is not supported in Oracle Standard Edition or Standard Edition One.*

CDN Backup

The Content Delivery Network is used to store distributed apps, documents and agent versions. Be sure to include it in your backup plan.

The CDN is hosted in the Services VM and is at /u002. Because the Services VM should be part of your VMware backup plan, the CDN is automatically included. However, it is possible to back up CDN content separately with a utility.

Prepare the CDN backup utility by completing the following steps:

1. Download the CDN backup script from the **Downloads** tab in the Administration Console. For more information, see MaaS360 Management Tools.

Note: *The **Downloads** tab might not be available within the Administration Console until you have configured your deployment.*

2. Copy and run the script on the server where you want to back up the CDN content. Specific CDN user credentials exist for this operation. The cdn user is the default user, and you are prompted for the password after the script runs:

User: *cdn*

Password: *MaaS360_Console*

Note: *The user who runs this script must have permissions to create subdirectories under the directory where the script is run.*

The cdnbackup.sh script can be used according to the following parameters to back up the CDN content:

```
cdnbackup.sh [-b<backup_dir>] [-l <remote_user>] [-H <remote_host>]
[-d <remote_dir>] [-D <dir_list>]
```

Where:

`-h` Help

`-b` Directory to back up. This parameter can be omitted if default value is used.

`-l` User login name. This parameter can be omitted when you use the default cdn user.

`-H` IP address of Services VM or host name, if a DNS entry can be added for the Services VM host name.

`-d` Base directory to back up from, can be omitted if default value is to be used.

`-D` List of directory names in CDN to be backed up, can be omitted if default value is to be used.

The following example command backs up the entire CDN to the specified backup server:

```
./cdnbackup.sh -H<service_VM_IP_address>
```

Note: *When prompted for a password, enter the cdn user password* MaaS360_Console.

IBM MaaS360 Cloud Extender and IBM MaaS360 Mobile Enterprise Gateway Backup

IBM MaaS360 Cloud Extender and IBM MaaS360 Mobile Enterprise Gateway are optional, but if either one is part of your deployment they must be part of your backup and recovery plan.

The entirety of your deployment must be backed up. This is most easily accomplished by deploying them on virtual machines and including the VMs in your backup plan. VMware vSphere Data Protection is the recommended tool for managing your VM environment backup and restoration needs.

Data Retention

IBM MaaS360 stores several types of data that are rotated or purged. A retention policy must be defined to retain relevant data.

Application Log Retention

Application logs are stored in the log directory. They are rotated after they reach 1 GB in size. Older logs are retained in the log directory and are not purged.

Application logs are accessible through the Administration Console. For more information, see Collect Application Logs.

Database Table Retention

Tables that grow quickly in size are purged daily at midnight based on their individual predefined retention schedule.

The following table outlines the database tables that are purged during the daily cycle. The purge policy for each table is based on the nature of the data in the table. The number of retention days for each table is predefined. Data in other tables that are not listed are retained indefinitely. All the purged tables are located in the VPN2 database.

Table 5. Database tables that are purged during the daily cycle

Table Name	Retention Days	Table Description
SCHEMA2.USER_BULK_ENROLLMENT_OPTS	32	This table is a log of enrollment options selected by the customer during the bulk upload user workflow.
SCHEMA2.USER_BULK_ACTIVATION_OPTS	32	This table is a log of activation options selected by the customer in the bulk upload users model box.
SCHEMA2.USER_BULK_UPLOAD_OPTS	32	This table is a log of upload options used by the DB job to process the record as a part of bulk upload users workflow.
SCHEMA2.USER_BULK_UPLOAD_QUEUE	32	This table contains transient queue data used for the bulk upload users workflow. It stores a list of all users from the uploaded file in the bulk upload users workflow.
SCHEMA2.USERS_AUDIT	180	Audit of actions performed in user management.
SCHEMA2.DEVICE_LOCATION_HST	97	History of locations of device that come in through payload data.
SCHEMA2.APP_DEV_NOTIFICATION_ASSOC	22	Stores document notification sent per device.
SCHEMA2.APP_NOTIFICATION_STAGE_1	22	This table is staging table used for notification stage 1. For example, when a document is shared this would have information about a notification is to the group to which the information is being shared. Expansion of it to individual devices would be done in APP_NOTIFICATION_STAGE_2.
SCHEMA2.APP_NOTIFICATION_OBJECT_COUNT	22	The number of notification objects to be stored with a single notification ID.
SCHEMA2.EVT_GRP_RE_EVAL_QUEUE	15	Transient data. Stores the device and OOC group information for consumption of group evaluation hence making it faster.
SCHEMA2.APP_CATALOG_INSTALL_IOS_HST	35	Install history logs of app catalog.
DEVICE_VIEW_APP.AUTH_RESPONSE_ATTRIBUTE	8	Stores authentication tokens required for web services, etc..
DEVICE_VIEW_APP.SERVICE_AUDIT_LOG	8	Stores access logs of service URLs.

Deployment Checklist

Print out the following list of steps and finish all of the tasks before starting the installation of IBM MaaS360.

Table 6. Deployment checklist

Task	Status
Database server is set up and root access credentials to database server are available.	
Database time zone is set to GMT.	
No idle timeout exists between MaaS360 VMs and the database server port.	
Database is running in archive mode for the RMAN backup.	
VMware server is set up with the ESXi vCenter Server and it is accessible from the vSphere client.	
Remote connectivity tools for the VMware host and database server are available.	
DNS entries for URLs have been created. These include Services, End User Portal, Enrollment URL, Portal URL, Gateway URL and Database virtual machine hosts.	
Network ports on the external firewall are configured and opened, as per the diagram in the Firewall Ports section.	
SSL Certificates for Services, End User Portal, Portal and Enrollment URLs are available. An iOS code signing certificate must also be available if you are using reverse proxy with http deployment.	
Password from SSL Certificate private keys has been removed.	
SMTP Server is set up and the hostname and port details are available.	
NFS Server is set up and it is accessible from the Services and Standalone VMs.	
Process of obtaining required certificates such as an Apple APNS certificate has begun.	
IBM MaaS360 Virtual appliance package (.OVA), and the Database Artifact package for Oracle should be downloaded from PPA.	
Optional: Apple iOS Code Signing Certificate has been procured. It is required if you want to manage iOS devices.)	
Optional: Symantec Windows Phone Code Signing Certificate has been procured. It is required if you want to manage Windows Phone devices.	

Database Installation

The first component of your IBM MaaS360 deployment that must be installed is your database infrastructure. For more information, see Deployment Architecture, Hardware Requirements, and Software and Network Requirements.

Before proceeding, an Oracle Database Server running version 11.2.0.4.0 should be configured and ready for creating new databases. You should also have the database artifacts file downloaded from IBM Passport Advantage®. The database artifacts are delivered as database templates. These templates were created using Oracle's Database Configuration Assistance (DBCA). DBCA is required to import the templates and create new databases on your server.

Note: *The database artifact includes installation scripts for Linux, AIX and Solaris platforms only. If you intend to use any other platform, review the scripts and rewrite them for the platform you have chosen.*

Important:

- *Ensure that the database server time zone has been set to GMT before proceeding further.*
- *Ensure that no idle time has been set between the MaaS360 VMs and the database server.*

Database Parameters

The database templates have default values associated with them.

Some of the database template default values can be overridden to suit your deployment, if necessary. Others must not be overridden.

Any parameters that are not listed below are set at Oracle default values. These values can be changed at your discretion.

The following database parameters **must not** be overridden:

- SID
- Character Set
- Database Name

The following database parameters can be overridden, if necessary:

- Archive log mode - Enable this parameter to allow database backup.
- Storage Type
- Storage Location
- Data Directory
- Faster Recovery Area (FRA) size and directory - If you choose to override the FRA size, ensure that the value is greater than the default.
- Sys and System User passwords
- PGA size
- SGA size components:
  - Shared pool
  - Buffer cache
  - Java™ pool

- Large pool

If you choose to override any of these memory parameters, ensure that the value is greater than the default:

- Number of processes - If you choose to override this parameter, ensure the value is greater than the default.
- Connection mode - **Dedicated** mode is recommended for best performance.

Note: *Enable Archive Log Mode for all four databases so that you can use RMAN.*

Database Template Deployment

With an Oracle environment set up, the IBM MaaS360 database template must be deployed to create four databases.

To deploy the IBM MaaS360 database artifacts, perform the following steps:

As the root user, check and update the following Oracle parameters at the OS level so they are **at least** at the values below:

Table 7. Oracle parameters

Parameter	Value
Maximum Open File Descriptors for user	Minimum: 50000
Maximum Processes Available for user	Minimum: 50000
Maximum Total Shared Memory (SHMMAX)	Minimum: 6442450944
Shared Memory Pages (SHMALL)	Minimum: 2097152

Note: *Perform the following steps as the system user that manages the Oracle database (typically the Oracle user).*

3. Copy the IBM MaaS360 Database Artifact package file that was obtained from Passport Advantage to the database server and extract the file.
4. Copy the following database template files from `<base folder>/11.2.0.4/` to the `assistants/dbca/templates` directory under `ORACLE_HOME`:

   - `agilink_clone.ctl`
   - `agilink_clone.dbc`
   - `agilink_clone.dfb`
   - `edw_clone.ctl`
   - `edw_clone.dbc`
   - `edw_clone.dfb`
   - `p03_clone.ctl`
   - `p03_clone.dbc`
   - `p03_clone.dfb`
   - `vpn2_clone.ctl`
   - `vpn2_clone.dbc`
   - `vpn2_clone.dfb`

5. Using DBCA, import the following templates. You can override the default values in the templates according to your environment in accordance with the rules described in Database Parameters.

   - agilink_clone
   - edw_clone
   - p03_clone
   - vpn2_clone

6. Edit the db_update.ini file in the extracted folder, and update the following parameters to values that fit the availability in your environment. Do not change the values of any other parameters.

   - ORACLE_HOME
   - DB_DOMAIN
   - APP_PASS – Change this only if you intend to change the default password for all DB users to a password of your choice.
   - DB_SYSTEM_PASS – Should be configured with **SYS** user password. SYS user password should be configured to be the same across VPN2, AGILINK, PO3 and EDW databases.

7. If the database management user is not the oracle user, you must edit the update_m360_databases.sh file in the extracted folder. Replace all references to zzoracle to zz<database_management_user>.

8. If Oracle RAC is used, modify the file update_m360_databases.sh:

   a. Update the following lines:

      - export ORACLE_SID=$AGILINK_SID: replace $AGILINK_SID with the correct Agilink database SID for the Oracle RAC node.
      - export ORACLE_SID=$VPN2_SID: replace $VPN2_SID with the correct VPN2 database SID for the Oracle RAC node.
      - export ORACLE_SID=$EDW_SID: replace $EDW_SID with the correct EDW database SID for the Oracle RAC node.
      - export ORACLE_SID=$P03_SID: replace $P03_SID with the correct P03 database SID for the Oracle RAC node.

   b. Modify the following line to include a storage clause as required by your environment. The following line occurs four times in update_m360_databases.sh; update each occurrence:

      - alter tablespace TEMP add tempfile size 100M autoextend on maxsize 4000M;

9. Create or edit network/admin/tnsnames.ora under ORACLE_HOME, and add or edit the following TNS names. Replace the bracketed values in each line with the correct values.

```
agilink=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(HOST=<ip_address_or_hostname>)(PORT=
<listner_port>)(PROTOCOL=TCP))(ADDRESS=(HOST=<ip_address_or_hostname>)(PORT=
<listner_port>)(PROTOCOL=TCP)))(CONNECT_DATA=(SID=<agilink_sid>)(SERVER=DEDICATED)))

vpn2=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(HOST=<ip_address_or_hostname>)(PORT=
<listner_port>)(PROTOCOL=TCP))(ADDRESS=(HOST=<ip_address_or_hostname>)(PORT=
<listner_port>)(PROTOCOL=TCP)))(CONNECT_DATA=(SID=<vpn2_sid>)(SERVER=DEDICATED)))

p03=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(HOST=<ip_address_or_hostname>)(PORT=
<listner_port>)(PROTOCOL=TCP))(ADDRESS=(HOST=<ip_address_or_hostname>)(PORT=
<listner_port>)(PROTOCOL=TCP)))(CONNECT_DATA=(SID=<p03_sid>)(SERVER=DEDICATED)))

edw=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(HOST=<ip_address_or_hostname>)(PORT=
<listner_port>)(PROTOCOL=TCP))(ADDRESS=(HOST=<ip_address_or_hostname>)(PORT=
<listner_port>)(PROTOCOL=TCP)))(CONNECT_DATA=(SID=<edw_sid>)(SERVER=DEDICATED)))
```

```
NODE_LISTENER=(DESCRIPTION=(ADDRESS=(HOST=<ip_address_or_hostname>)(PORT=
<listner_port>)(PROTOCOL=TCP)))

REMOTE_LISTENER=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(HOST=
<ip_address_or_hostname>)(PORT=<listner_port>)(PROTOCOL=TCP))(ADDRESS=(HOST=
<ip_address_or_hostname>)(PORT=<listner_port>)(PROTOCOL=TCP))))
```

10. Create or edit `network/admin/listener.ora` under `ORACLE_HOME` and add or edit the following line:

```
LISTENER=(DESCRIPTION=(ADDRESS=(HOST=<i/p address / hostname>)(PORT=
<listner_port>)(PROTOCOL=TCP)))
```

11. Stop the Oracle database and listener if they are already running and restart the database only.
12. Execute `update_m360_databases.sh`, to perform post installation updates to the databases. If any errors are reported, they have to be corrected before you proceed further.
13. Restart the Oracle database listener.
14. Execute `validate_database_setup.sh`, to perform a validation of the database installation and configuration.
    If any errors are reported, they have to be corrected before you proceed further.

Note: *Do not proceed with the Instance Configuration through the MaaS360 Administration Console unless all errors reported by the validation script have been resolved.*

IBM MaaS360 Virtual Appliance

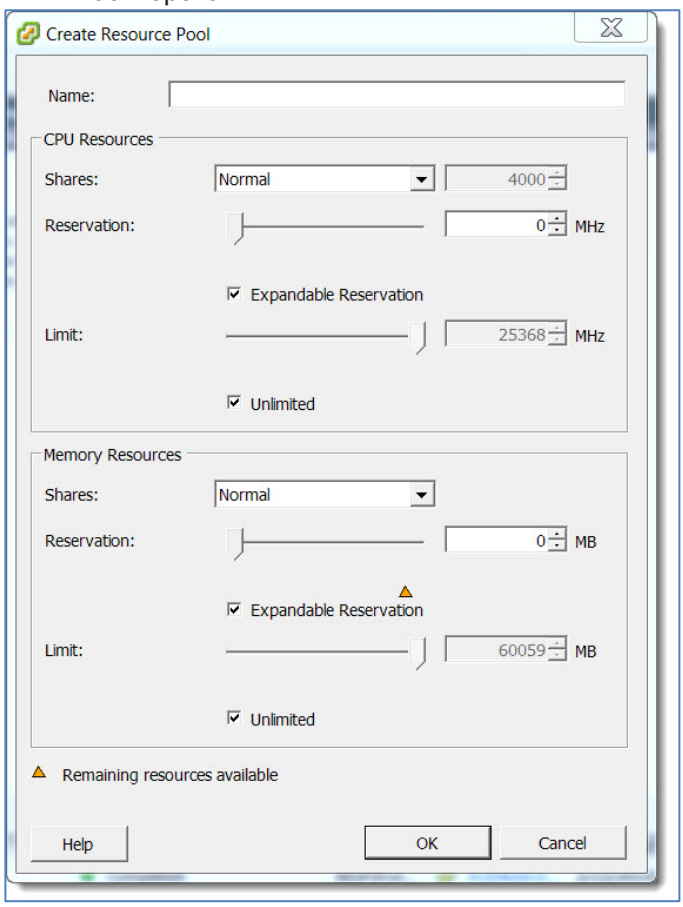
IBM MaaS360 is deployed as a VMware Virtual Appliance, or vApp, on an ESXi server or ESXi cluster. The vApp contains several virtual machines that constitute the bulk of your IBM MaaS360 deployment.

Create a Resource Pool

A VMware resource pool is a pre-requisite for the successful deployment of the vApp in a VMware Cluster. You can use an existing resource pool or deploy one from the VMware vSphere client.

To deploy a resource pool, perform the following steps from the vSphere client, which must be connected to your VMware Virtual Center:

1. Navigate to the ESXi host designated for your IBM MaaS360 vApp deployment using the VMware vSphere client.
2. Right-click and select **New Resource Pool** from the drop-down menu. The **Create Resource Pool** window opens.



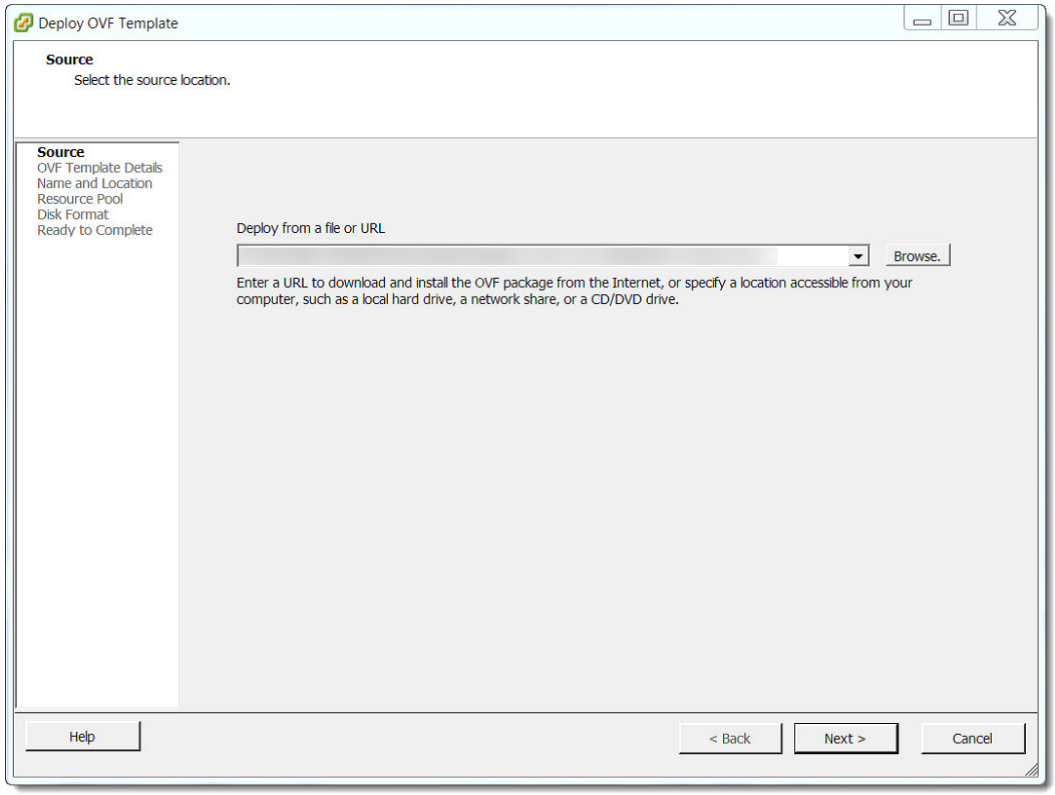
3. Enter a name for the Resource Pool, and enter values appropriate for your VMware environment.

Deploy the vApp

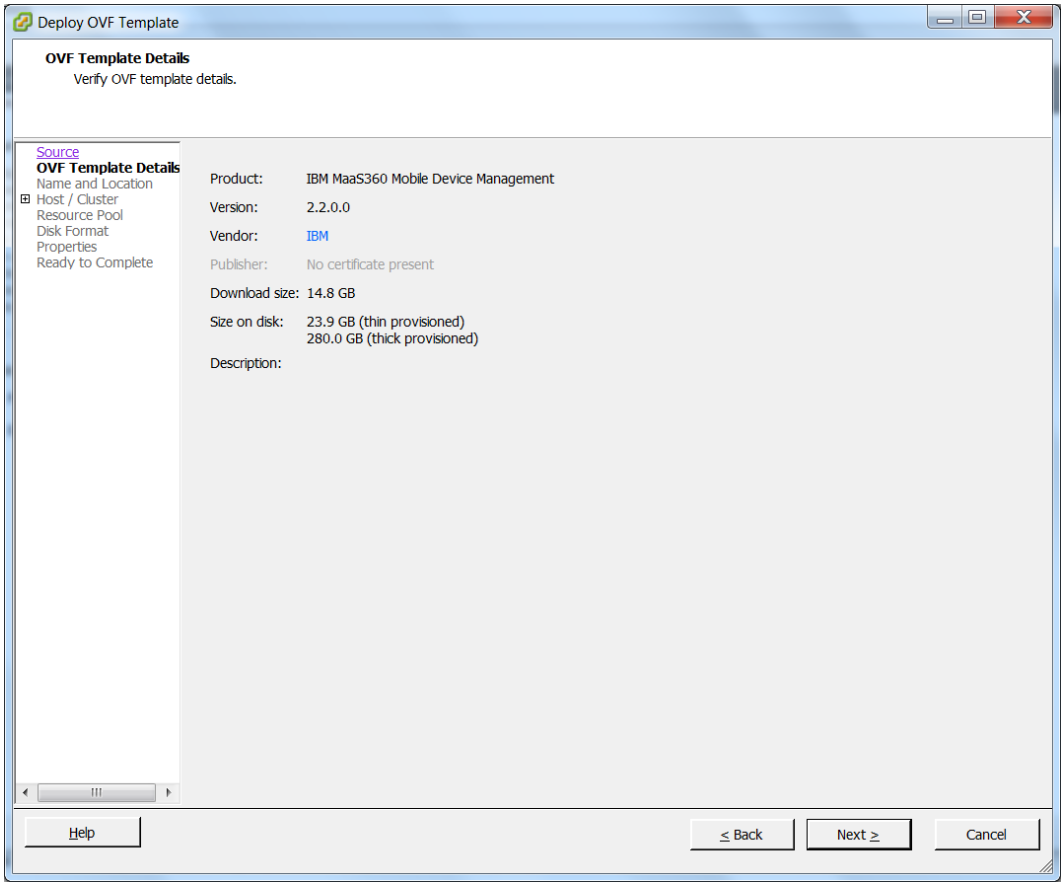
After creating a resource pool, the vApp must be imported and configured.

From the vSphere Client, connect to your VMware Virtual Center and perform the following steps:

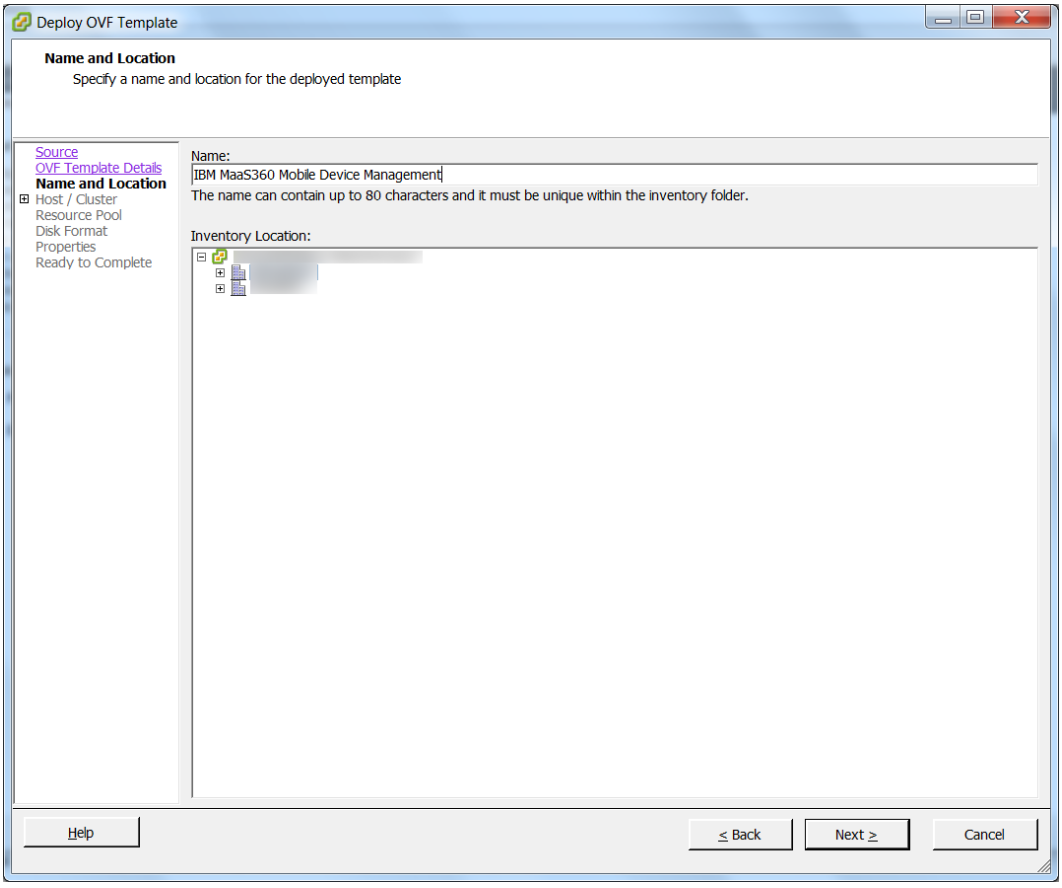
1. Select the relevant resource pool on the left navigation panel where you will import the IBM MaaS360 vApp.
2. From the **File** menu, click **Deploy OVF Template**. The **Deploy OVF Template** screen opens.



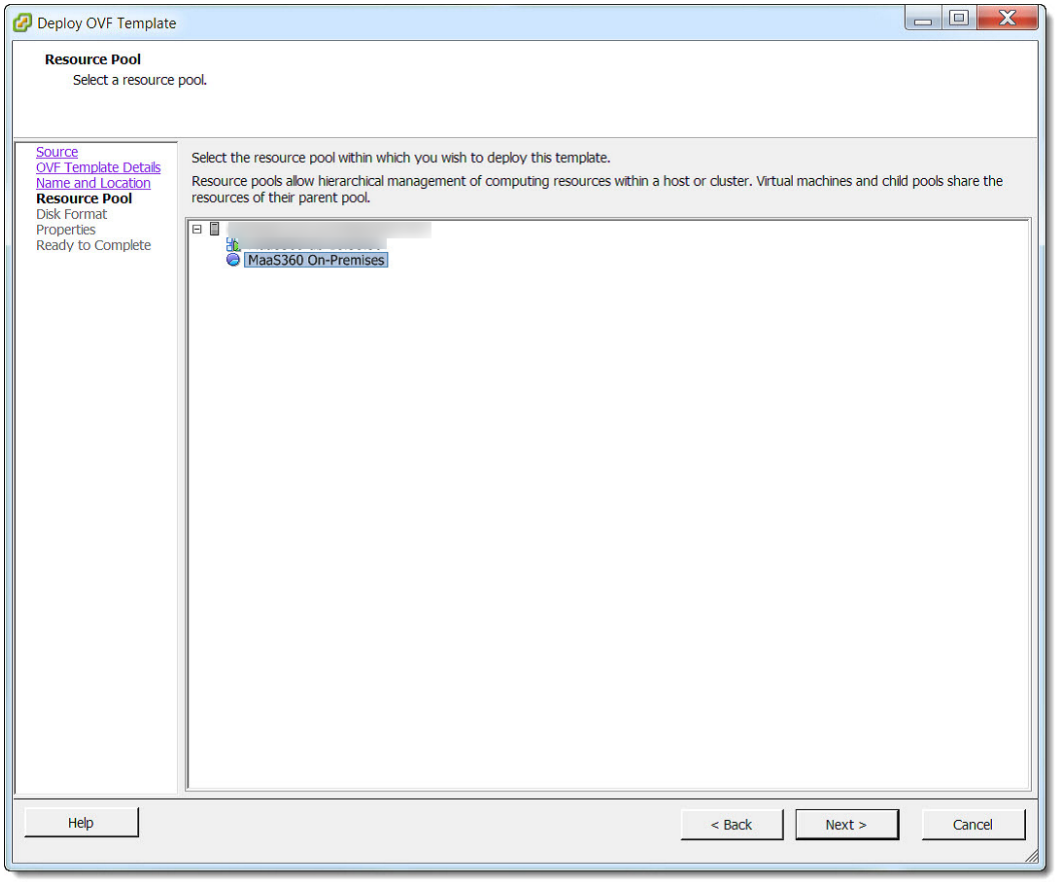
3. Click **Browse** and navigate to the location of the OVA file. Select the OVA file and click **Next** to view the **OVF Template Details** window.



4. Click **Next** to display the **Name and Location** screen. You can edit the name of the vApp. Select the appropriate inventory location and click **Next**.

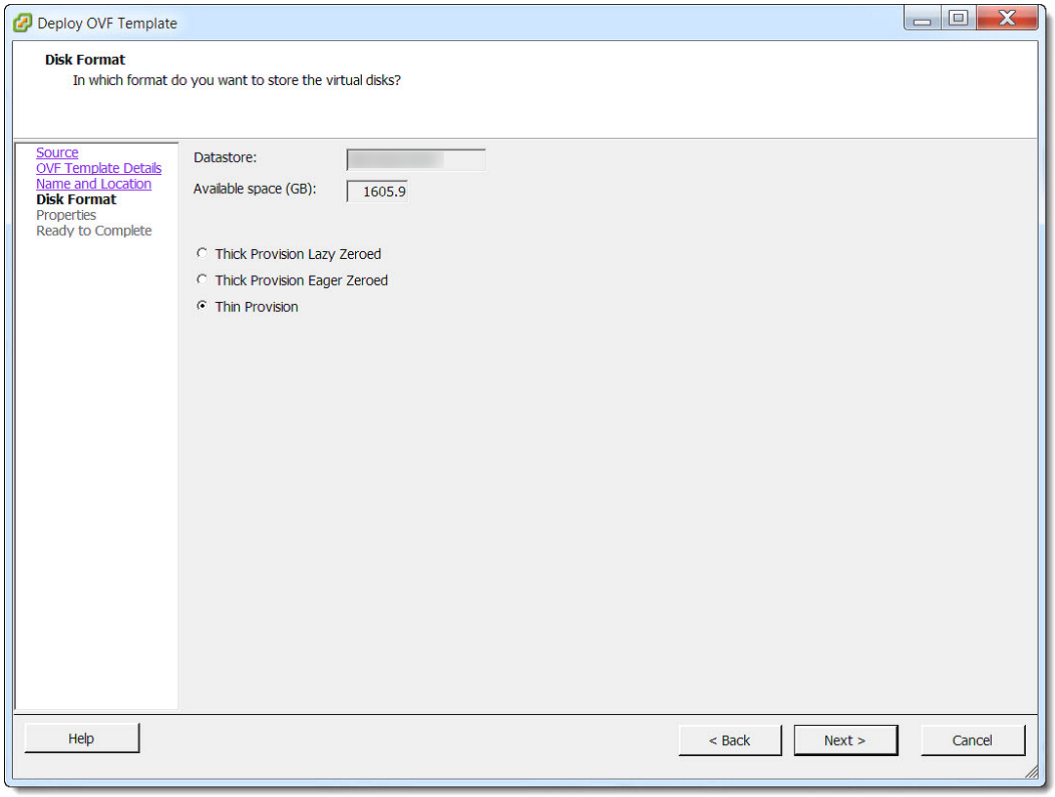


5. If you did not select the newly created resource pool when deploying the template, you will be asked to designate a resource pool. Click **Next** to proceed or skip this step.

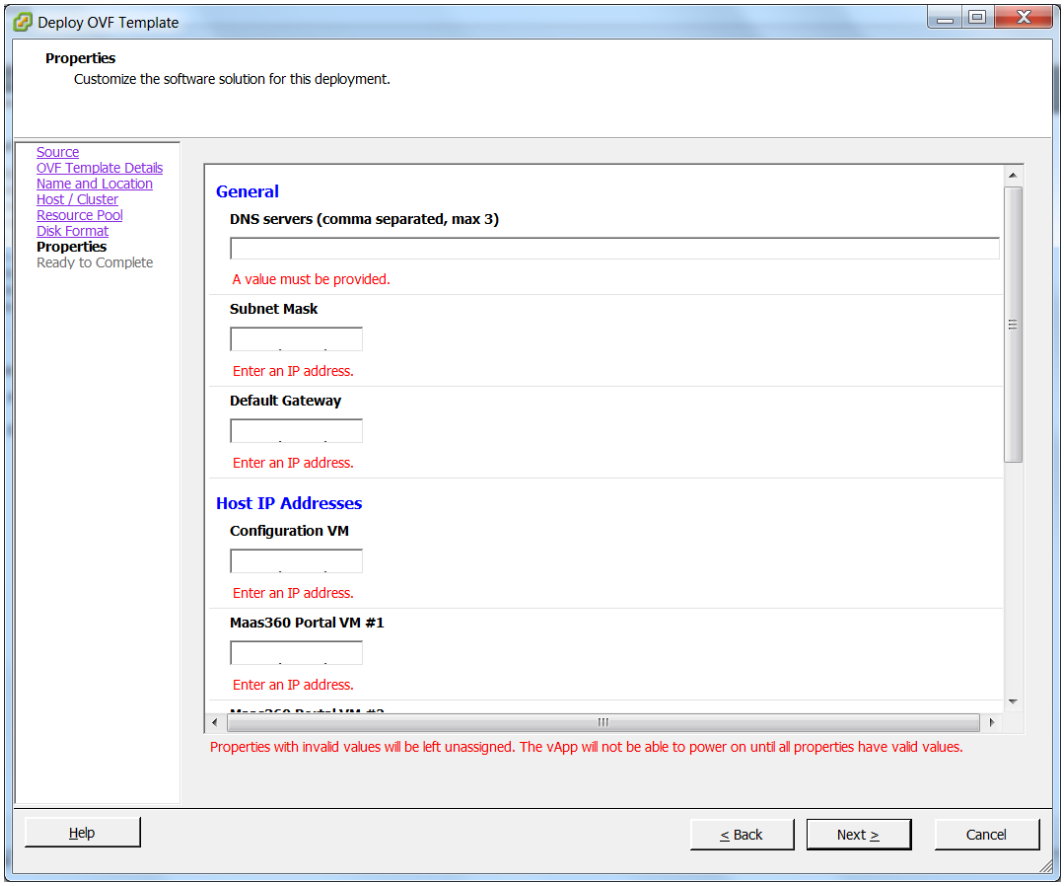


6. If multiple storage resources are available, the **Storage** screen allows you to select the storage resource for hosting the virtual appliance. If you are configuring your deployment for High Availability, select **shared storage**. Click **Next** to proceed. If only one storage resource is configured, this step is skipped.

7. The **Disk Format** screen displays the data store details for importing the appliance. **Thick Provision** is the recommended setting for better capacity planning. Click **Next** to proceed.



8. The **Network Mapping** screen maps the network that the virtual appliance must use. If there is only one network port group configured, this step may not show up during the import process. Select the relevant destination network(s) from the **Destination Networks** drop-down list. Click **Next** to proceed.
9. The **Properties** screen allows you to define several parameters of the vApp deployment.
    a. Under General, enter the IPs for the following components in the network in which the vApp is deployed:
        - DNS Servers: MaaS360 vApp should have access to the DNS Gateway that is required to look up the external DNS URL entries.
        - Subnet Mask
        - Default Gateway



b. Under the **Host IP Addresses** heading on the same screen, enter the internal IP addresses reserved for the seven virtual machines. For more information, see Network Configuration.

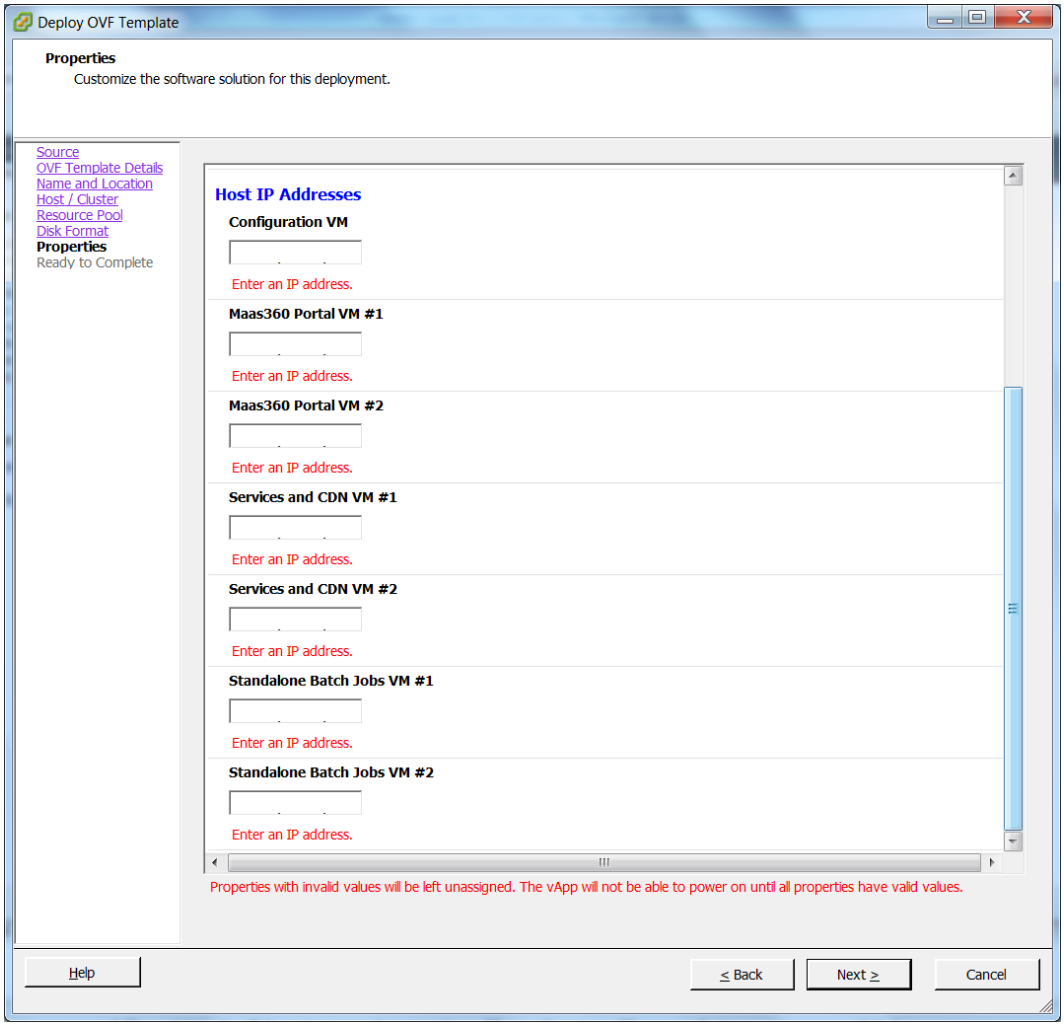
- Configuration VM
- IBM MaaS360 Portal VM #1—node 1 of the Portal VM
- IBM MaaS360 Portal VM #1—node 1 of the Portal VM
- IBM MaaS360 Services and CDN VM #1—node 1 of the Services VM
- IBM MaaS360 Services and CDN VM #2—node 2 of the Services VM
- IBM MaaS360 Standalone Batch Jobs VM #1—node 1 of the Standalone Batch Jobs VM
- IBM MaaS360 Standalone Batch Jobs VM #2—node 2 of the Standalone Batch Jobs VM

Note: *All seven IP addresses must be valid to deploy the vApp in native High Availability mode.*

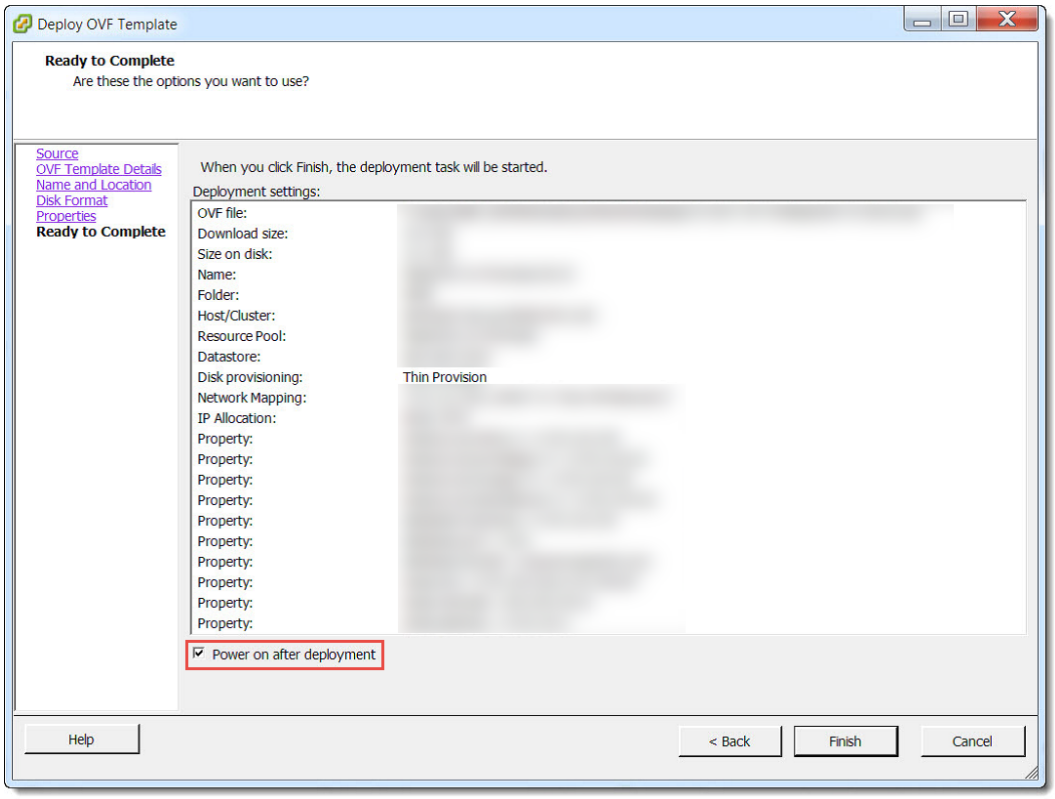
To deploy it in non-native High Availability mode, enter valid IP addresses for the following:

- IBM MaaS360 Configuration VM
- IBM MaaS360 Portal VM #1
- IBM MaaS360 Services and CDN VM #1
- IBM MaaS360 Standalone Batch Jobs VM #1

You could enter 255.255.255.255 for the IP addresses of the IBM MaaS360 Portal VM #2, IBM MaaS360 Services and CDN VM #2 and IBM MaaS360 Standalone Batch Jobs VM #2. These Node 2 VMs will not be in use in non-native High Availability mode.


Deploy OVF Template
Properties
Customize the software solution for this deployment.
Source
OVF Template Details
Name and Location
Host / Cluster
Resource Pool
Disk Format
Properties
Ready to Complete
Host IP Addresses
Configuration VM
Enter an IP address.
Maas360 Portal VM #1
Enter an IP address.
Maas360 Portal VM #2
Enter an IP address.
Services and CDN VM #1
Enter an IP address.
Services and CDN VM #2
Enter an IP address.
Standalone Batch Jobs VM #1
Enter an IP address.
Standalone Batch Jobs VM #2
Enter an IP address.
Properties with invalid values will be left unassigned. The vApp will not be able to power on until all properties have valid values.
Help
< Back
Next >
Cancel

10. Click **Next** to view the **Ready to Complete** screen. This screen summarizes the different deployment settings. Confirm all of the settings before the vApp import starts. If necessary, click **Back** to return to the previous screen to change any settings.

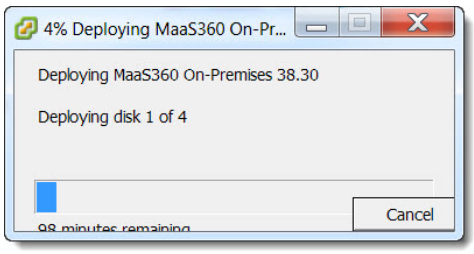


11. Select the **Power on after deployment** checkbox.

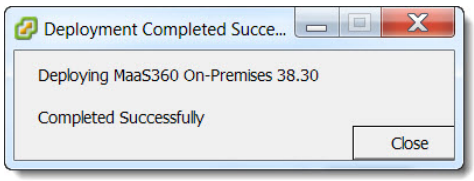
Note: *If you are deploying the vApp in non-native High Availability mode, clear this checkbox instead.*

12. Click **Finish** to continue with the deployment process. A bar will show the progress and time remaining for the process to finish.

    It might take more than an hour for this process to run.



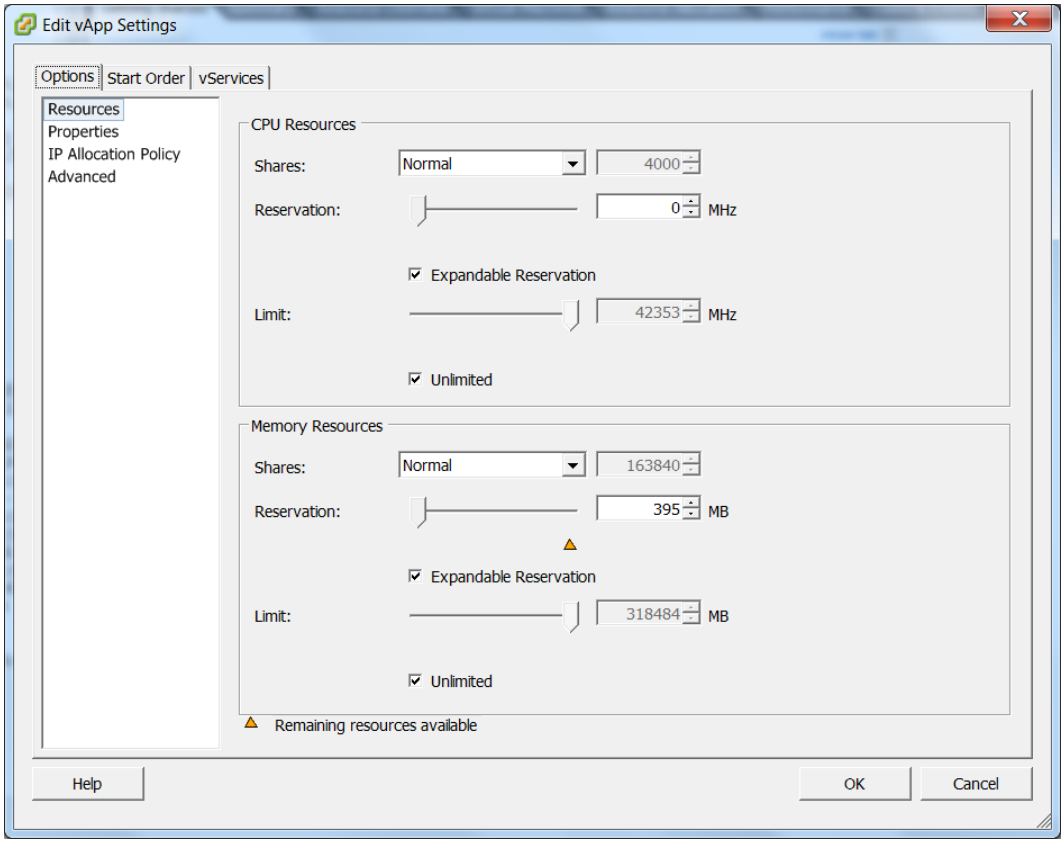
13. You will receive a success message if the deployment has completed successfully.



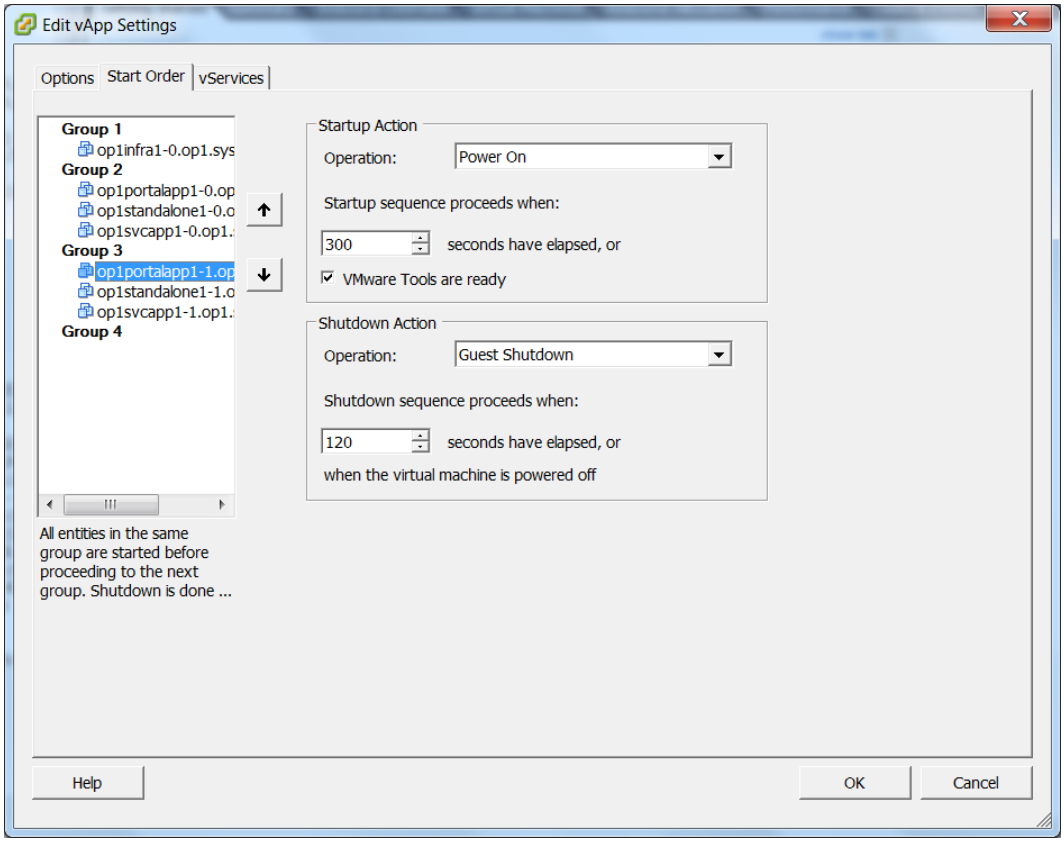
14. If you have deployed the vApp in native High Availability mode, skip this Step and proceed to Step #15:

    Stop Power On operation for Node 2 VMs for non-native High Availability mode deployment.

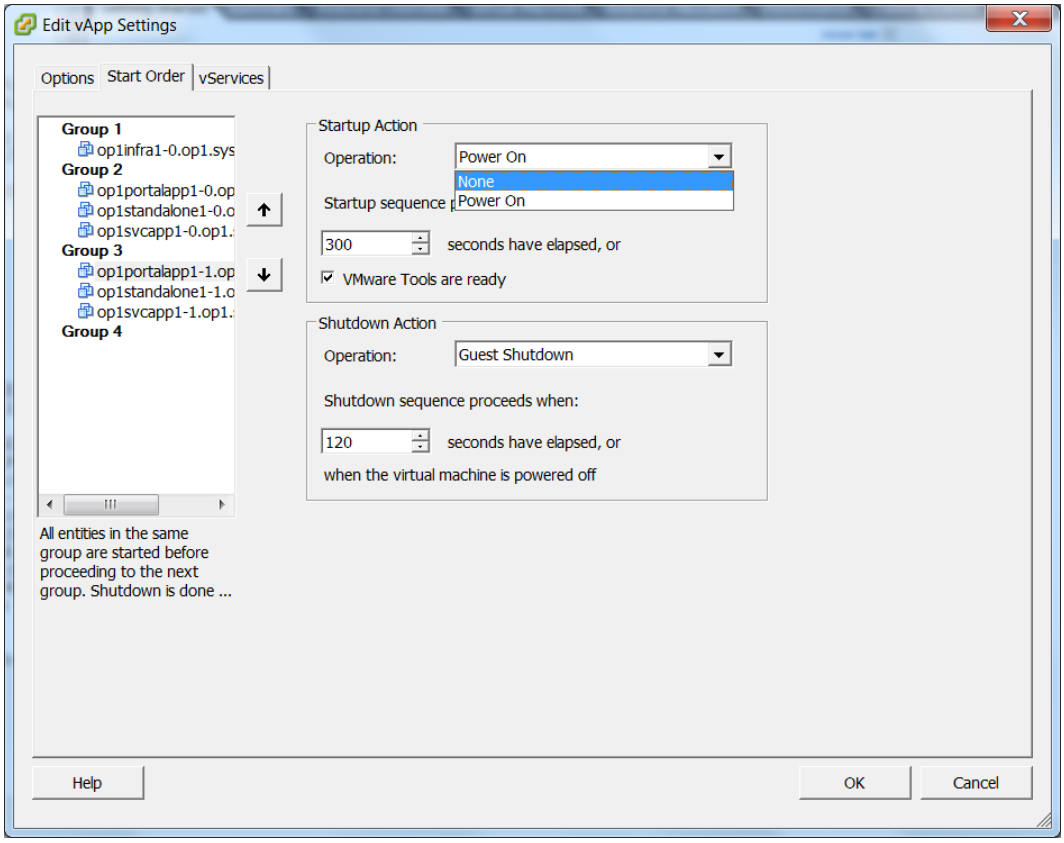
- Click on the deployed vApp in the vCenter and select **Edit vApp Settings**.



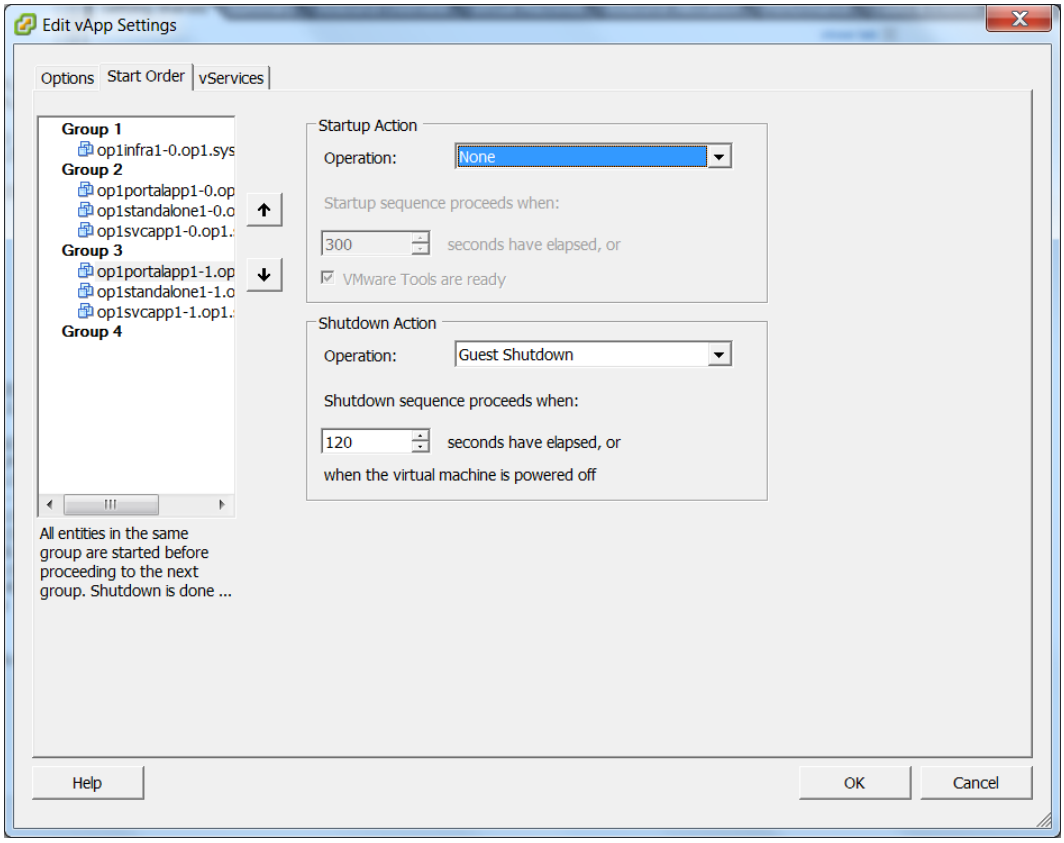
15. Click the **Start Order** tab and select the VMs in **Group 3**.



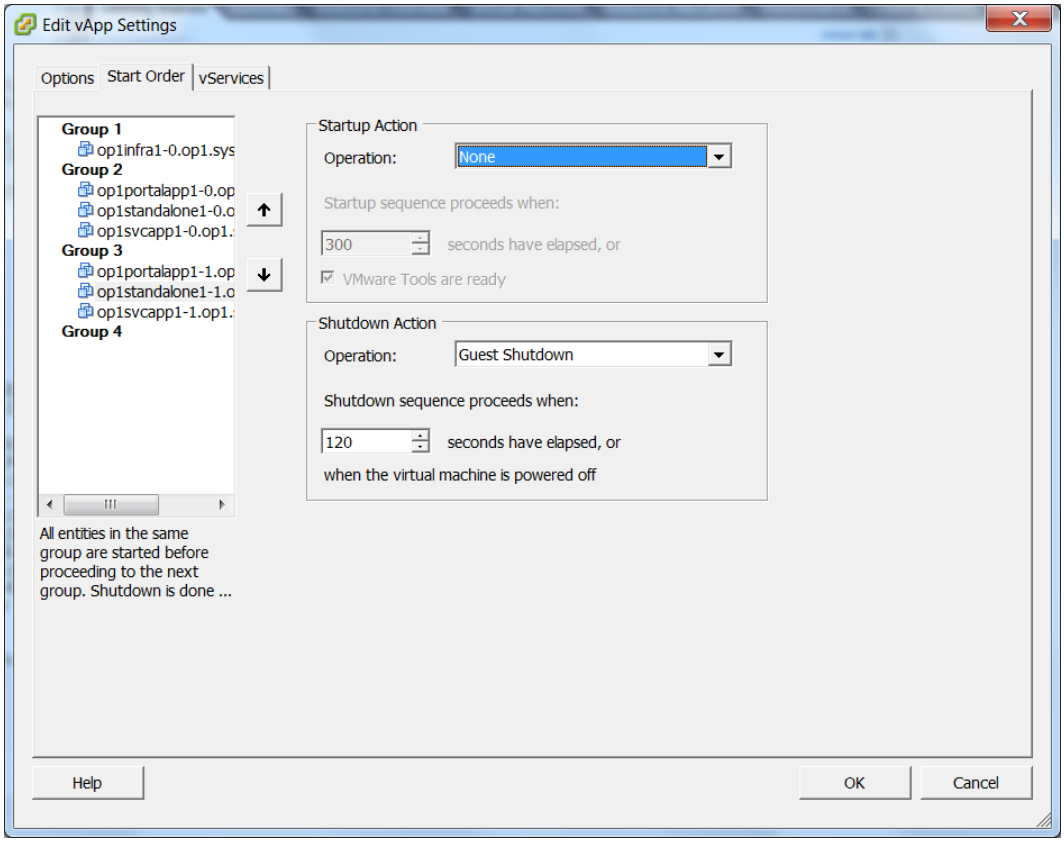
16. Change the **Startup Action > Operation** to *None* for each of the three VMs in **Group 3**.



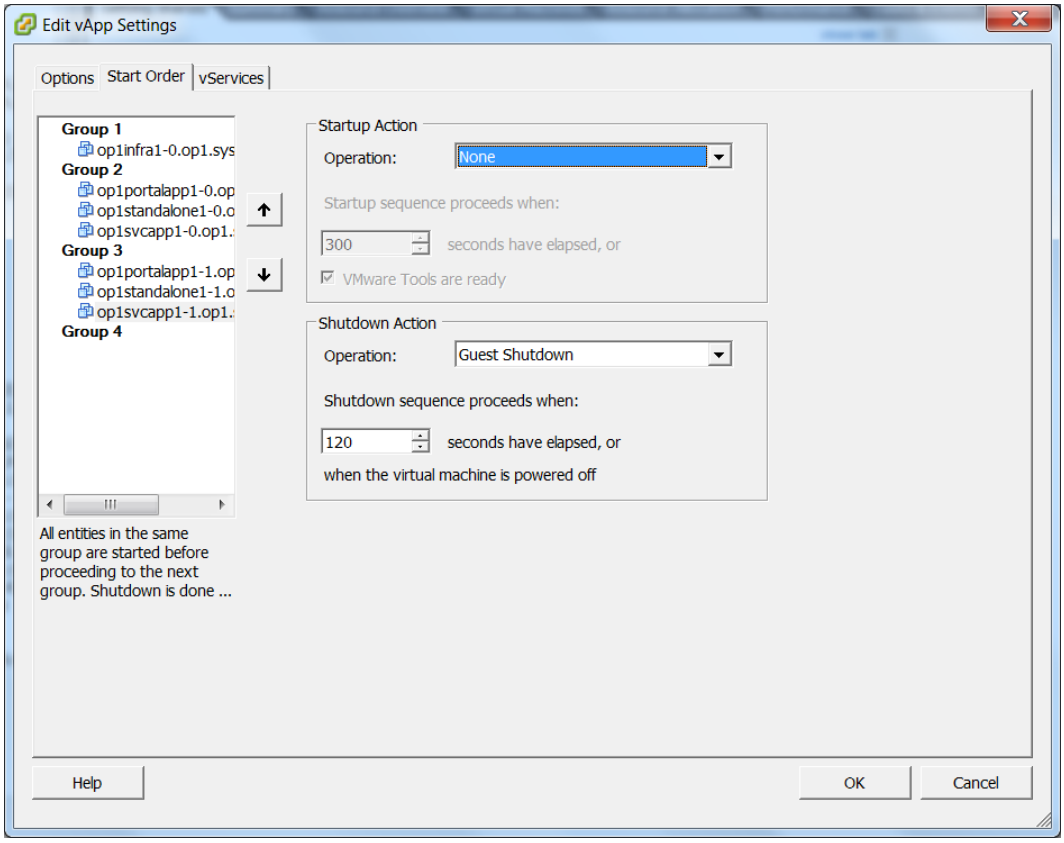
Here's what the Portal 1-1 VM will look like with the **Startup Action > Operation** set to *None*.



Here's what the Standalone 1-1 VM will look like with the **Startup Action > Operation** set to *None*.



Here's what the Services 1-1 VM will look like with the **Startup Action > Operation** set to *None*.



17. Click **OK** to save the changes.
18. Power on the vApp, and verify that only the VMs in Group 1 and Group 2 have been powered on.

Time Synchronization

Ensure the VMware ESXi hosts and Oracle database servers are hooked up to a common NTP server. You must keep the VMs and databases in sync with respect to time.

Deploying the vApp in a VMware Cluster

The vApp has seven virtual machines as follows:

Table 7. Node 1 and Node 2 VMs

VM Description	VM Host Name
Configuration VM	op1infra1-0.op1.sysint.local
Portal VM	op1portalapp1-0.op1.sysint.local op1portalapp1-1.op1.sysint.local

VM Description	VM Host Name
Services and CDN VM	op1svcapp1-0.op1.sysint.local op1svcapp1-1.op1.sysint.local
Standalone Batch Jobs VM	op1standalone1-0.op1.sysint.local op1standalone1-1.op1.sysint.local

For a native High Availability deployment you should deploy the vApp across ESXi Servers in an ESXi cluster. There should be a minimum of two ESXi Servers in the cluster.

Note: *VMware Distributed Resource Scheduler (DRS) module will be required to complete the setup explained below.*

Ensure the following are placed in the first ESXi host or host group:

- Configuration VM
- Portal VM - op1portalapp1-0.op1.sysint.local
- Services and CDN VM - op1svcapp1-0.op1.sysint.local
- Standalone Batch Jobs VM - op1standalone1-0.op1.sysint.local

Ensure that the following are placed in the second host or host group:

- Portal VM - op1portalapp1-1.op1.sysint.local
- Services and CDN VM - op1svcapp1-1.op1.sysint.local
- Standalone Batch Jobs VM - op1standalone1-1.op1.sysint.local

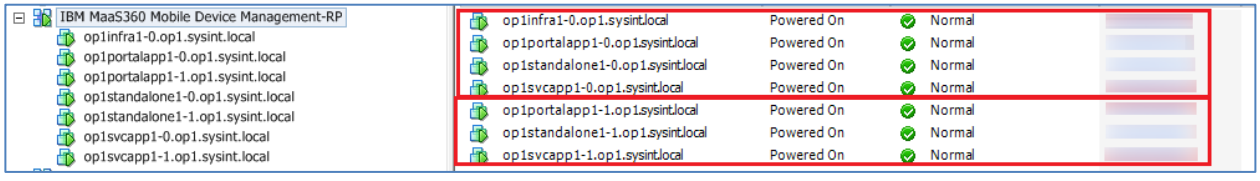
This will ensure uninterrupted availability of the VMs in case of failure of VMs on a single host or failure of the entire host. Ensure no 1-0 VM coexists with its corresponding 1-1 VM on the same host or host group.

To achieve this you should:

1. Create a DRS-enabled VMware cluster and deploy the vApp on this cluster.
2. Create two DRS cluster VM groups and place the 1-0 VMs in the first group and 1-1 VMs in the second group.
3. Create two DRS cluster Host groups containing one or more distinct ESXi hosts.
4. Create Rules to assign the first VM group to first host group and the second VM group to second host group.

This configuration will ensure there is no single point of failure and is the recommended configuration for MaaS360 native High Availability deployment.

Here is a sample configuration showing the 1-0 and 1-1 VMs placed on different ESXi hosts.



Refer to VMware's *vSphere Resource Management* for details.

Administration Console Configuration

After the IBM MaaS360 virtual appliance has been installed, the next step is to configure the deployment.

Configuration is performed by logging into the IBM MaaS360 Administration Console, or MAC, through a browser.

Before proceeding, ensure that the certificates and network requirements have been met as described in Software and Network Requirements. This procedure can take approximately two hours to complete.

Note: *If you are using Internet Explorer, version 11+ is required.*

Access the Administration Console

You can access the Administration Console using any browser.

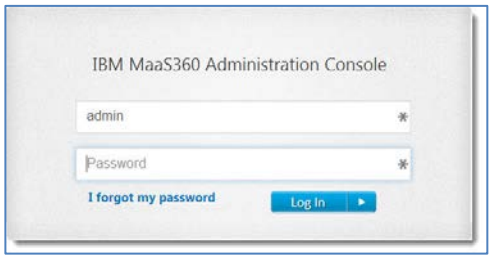
The Administration Console is hosted on the Configuration VM.

Access the MaaS360 Administration Console by completing the following steps:

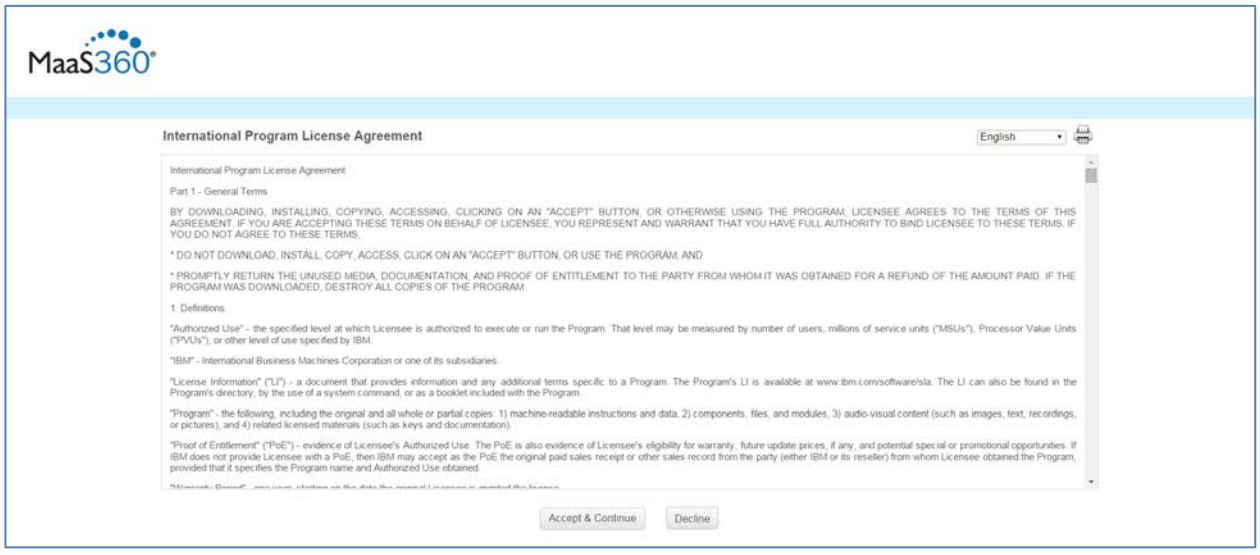
1. Using any browser, navigate to `http://<Configuration_VM>`. You might be presented with a warning that the address is untrusted, but this warning can be ignored.
2. Enter the default username and password and click **Log In**.

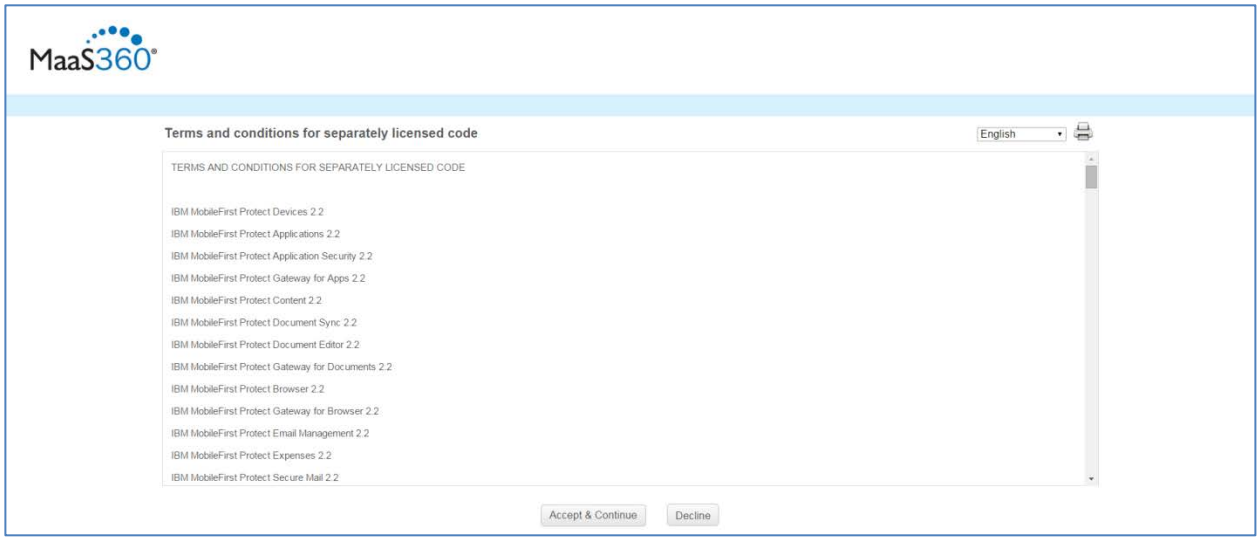
   User: *admin*

   Password: *manage*



3. You are presented with a series of license agreements. Accept the agreements to continue.





Deployment Mode

After accepting the license agreements, the **Deployment** screen is displayed.

MaaS360 can be deployed in the following ways:

1. Native High Availability mode along with an external load balancer

   You can choose to offload/terminate SSL at the load balancer or do it in MaaS360 vApp.

   A trusted SSL domain certificate has to be installed in the load balancer.

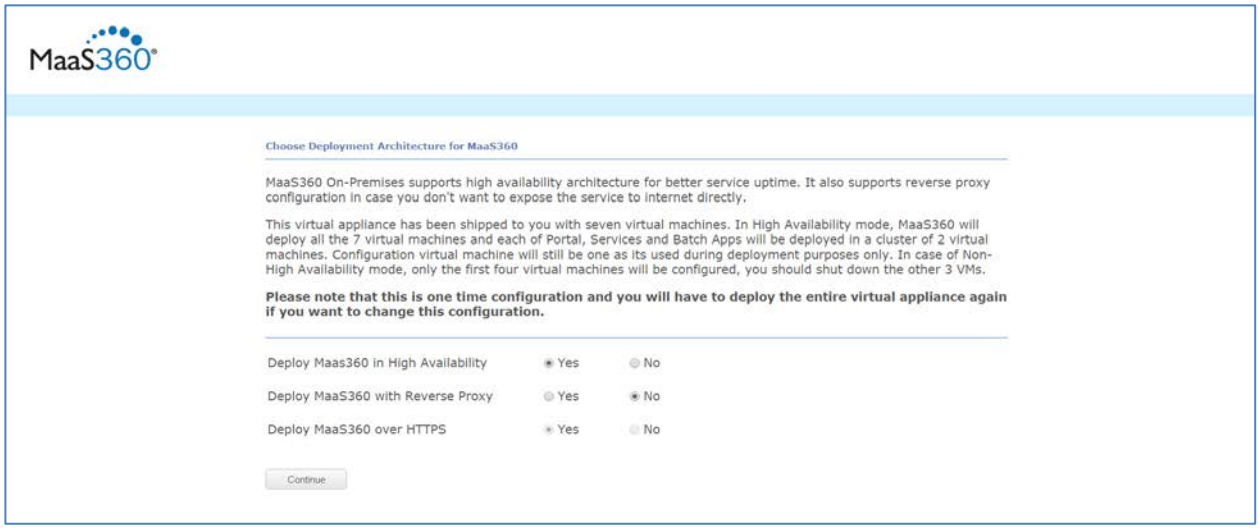
2. Non–native High Availability mode

   In this mode native High Availability is turned off and you should use VMware's High Availability capability in case you still need high availability.

3. Behind an external Reverse Proxy

   An external reverse proxy can shield MaaS360 vApp from direct interaction with the Internet. You have to offload/terminate SSL at the reverse proxy. You can either initiate http or https communication from the reverse proxy to the MaaS360 VMs.

   A trusted SSL domain certificate has to be installed in the reverse proxy.

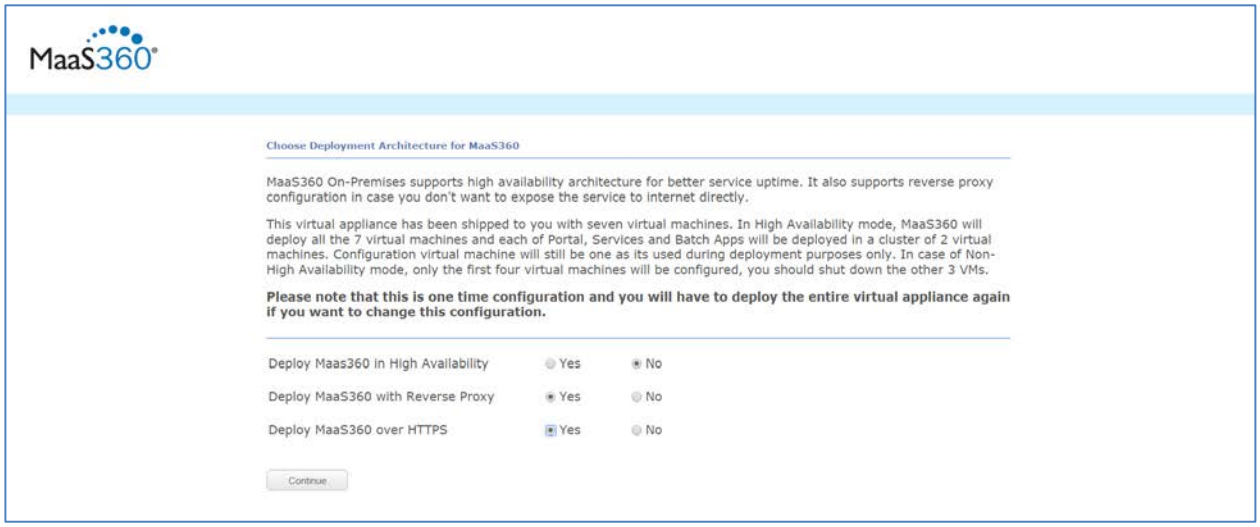


Important:

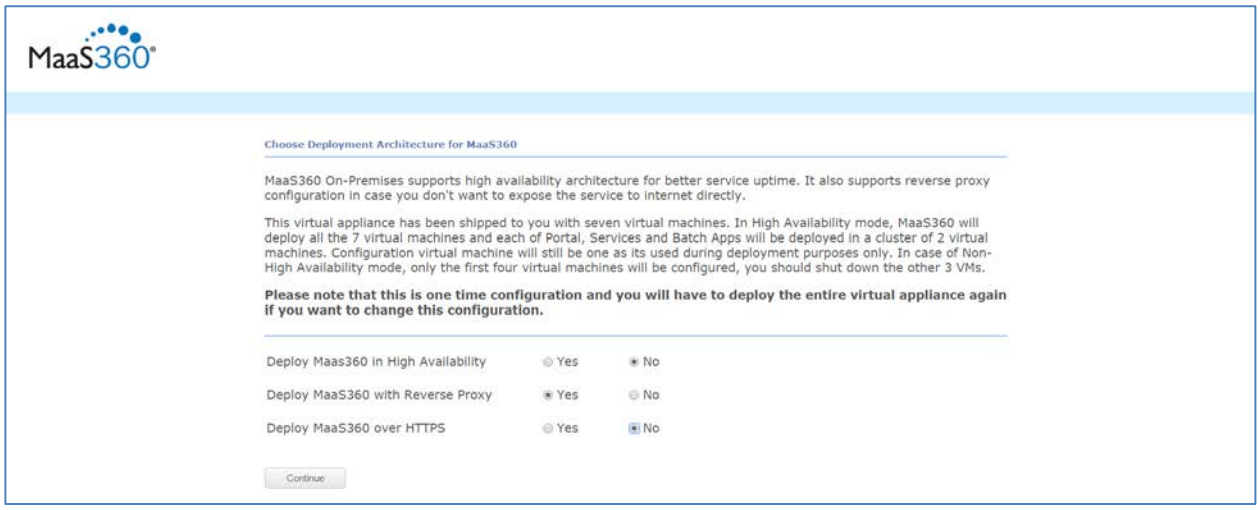
- **Please make sure you have read and understood the various ways MaaS360 can be deployed. You should then choose the deployment architecture based on your requirements and configure the instance according to the instructions below.**

Deploy MaaS360 in High Availability	• *Yes*—turn on the native High Availability feature • *No* (default)—turn off the native High Availability feature and deploy the vApp in non–native High Availability mode.
Deploy MaaS360 with a Reverse Proxy	• *Yes*—integrate the vApp with an external Reverse Proxy • *No* (default)—disable integration with an external Reverse Proxy
Deploy MaaS360 over HTTPS	This is only valid if you selected *Yes* for integration with Reverse Proxy. • *Yes*—offload or terminate SSL at the Reverse Proxy, and then use another SSL certificate to encrypt the traffic and forward HTTPS requests to the MaaS360 vApp (for enhanced security) • *No* (default)— offload or terminate SSL at the Reverse Proxy and then forward HTTP requests to the MaaS360 vApp

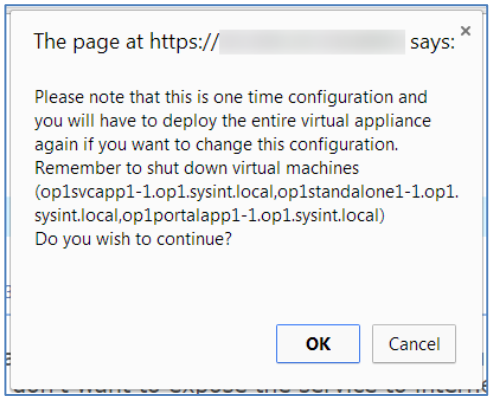
Selection for Reverse Proxy with https traffic routed to MaaS360 VMs:



Selection for Reverse Proxy with http traffic routed to MaaS360 VMs



Click **Continue**.



Important:

- Please review the above message carefully before you continue further.
- The deployment settings chosen above are irreversible for the life time of the instance. For example, if you have chosen the *native High Availability* option and later want to change that to *non – native High Availability*, you cannot. If these deployment settings must be changed, you have to redeploy the entire instance.
- If you choose the *non-native High Availability* option, you should shut down the Node 2 VMs by following instructions in Deploy the vApp.

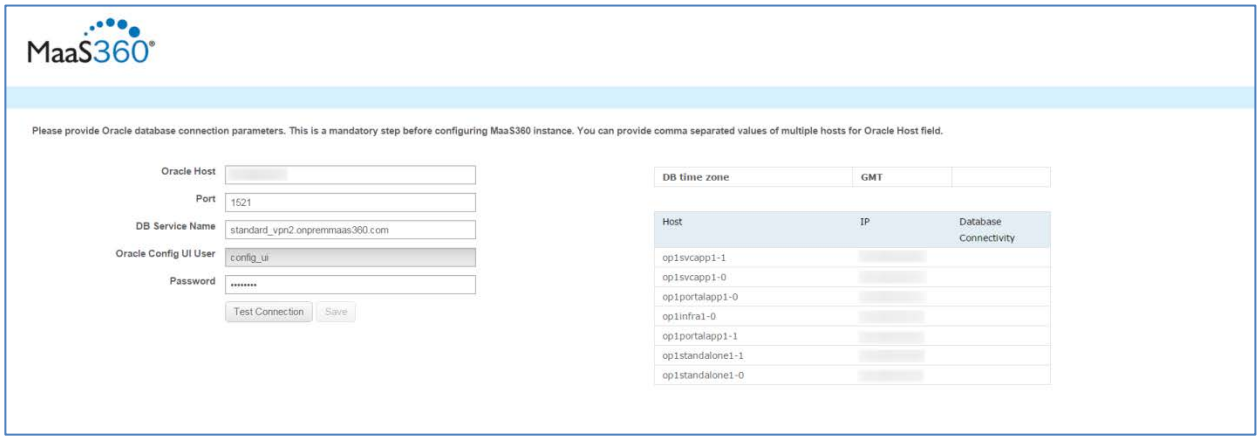
Click **OK** if you are sure of the chosen deployment settings to continue.

Click **Cancel** if you want to go back and review the deployment settings.

Database Configuration

Enter the following values:

Oracle Host	This is the hostname of IP address of your Oracle database. For an Oracle RAC setup, you can enter the hostnames or IP addresses of all your RAC nodes, separated by commas. ***Note:*** *It is a best practice to use the hostname alias instead of the IP address.*
Port	The database port. The default value is 1521.
DB Service Name	Enter it as `standard_vpn2.<DB_DOMAIN>` Enter the database domain you specified during your Oracle database installation for IBM MaaS360. This should be same as the domain value entered for the `DB_DOMAIN` parameter in the `db_update.ini` file used during database set up.
Password	Enter the password for your database deployment. This should be same as the password value specified for the `APP_PASS` parameter in the `db_update.ini` file used during database set up.



Verify that correct values have been entered and then click **Test Connection**.

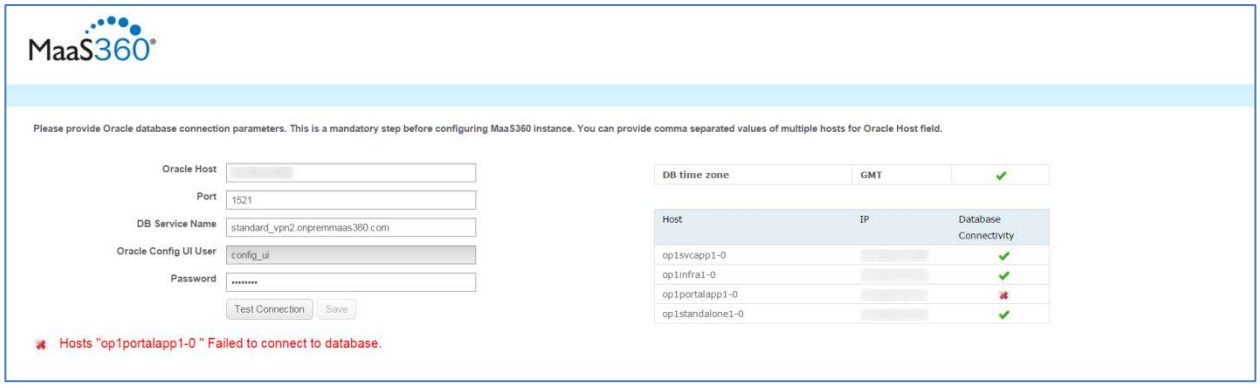
The database connection will be checked.

If database is not reachable from the Configuration VM or if any of the other VMs in the vApp are unable to connect to the database, you will see an error message.

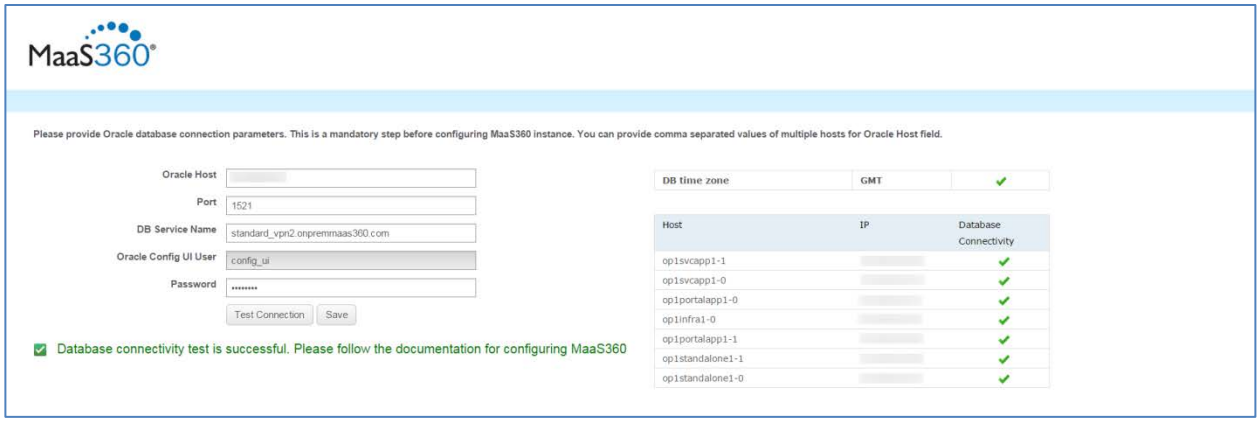
The status of the database connectivity for all the VMs is displayed on the right hand side of the screen. You cannot proceed unless all tests show a green checkmark.

Note: *Please make sure the database time zone is set to GMT. In the graphic below, the database time zone test is successful. If this shows an error, check the time zone at the database level and ensure it is set to GMT before you proceed further with the configuration.*

The graphic below shows a case where the Portal VM is unable to connect to the database.



After correcting all errors click on **Test Connection** again. Repeat this process till you see green checkmarks for all tests.



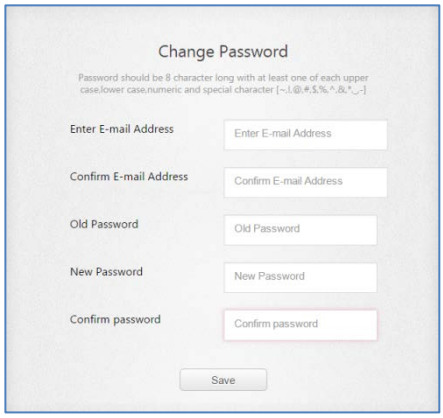
When all test are successful, the **Save** button will be enabled. Click it to persist the database connection and configure the connections.

Note: *This process may take up to 15 minutes to finish. Do not refresh the page.*

Change Password

The **Change Password** box will appear. You will be prompted to set a new password for increased security. Follow the specified guidelines.

You must also enter a valid email address. If you forget your password, a newly generated password can be sent to that address as part of the password reset process.



Click **Save** to continue.

Administration Console Navigation

Three tabs determine the configuration settings that are visible. The **Configure**, **Passwords**, and **Patches** icons are located in the upper-right corner of the user interface.

Configure

The bulk of your deployment configuration is performed using this tab. To begin the Administration Console configuration, see Solution Branding.

Passwords

This tab allows the configuration of the operating system passwords for the seven virtual machines contained in the IBM MaaS360 virtual appliance.

IBM MaaS360 also allows you to grant remote access to your IBM MaaS360 environment to IBM support. This access can be granted and revoked from the **Passwords** interface.

IBM MaaS360 also allows you to update the password applications used to connect to databases. This can be achieved through the **Database Password** link under **Passwords** interface.

Note: *It is highly recommended to update the password for the databases before they expire. For more information about the Passwords tab, see* Passwords.

Patches

This tab allows the deployment of new patches to fix issues with your instance. For more information, see Patches.

There are three icons under those tabs.

About

Displays version information for the various components of the deployment.

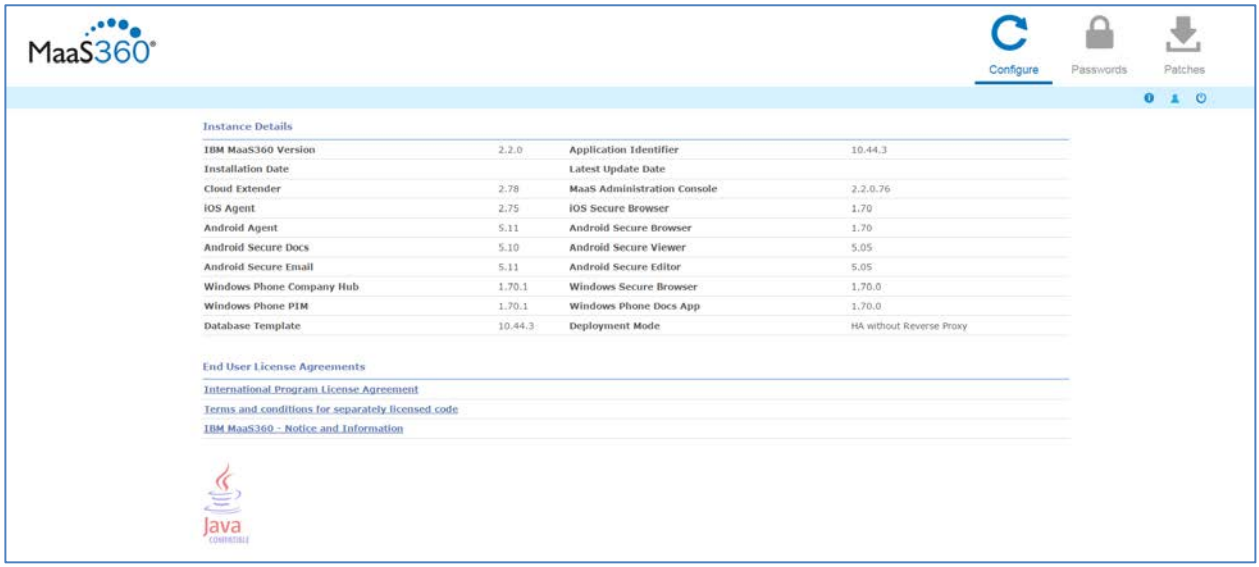
User

Displays the current user and allows that user's password to be changed. It also allows that user to log out of the configuration.

Logout

Logs the current user out of the configuration UI.

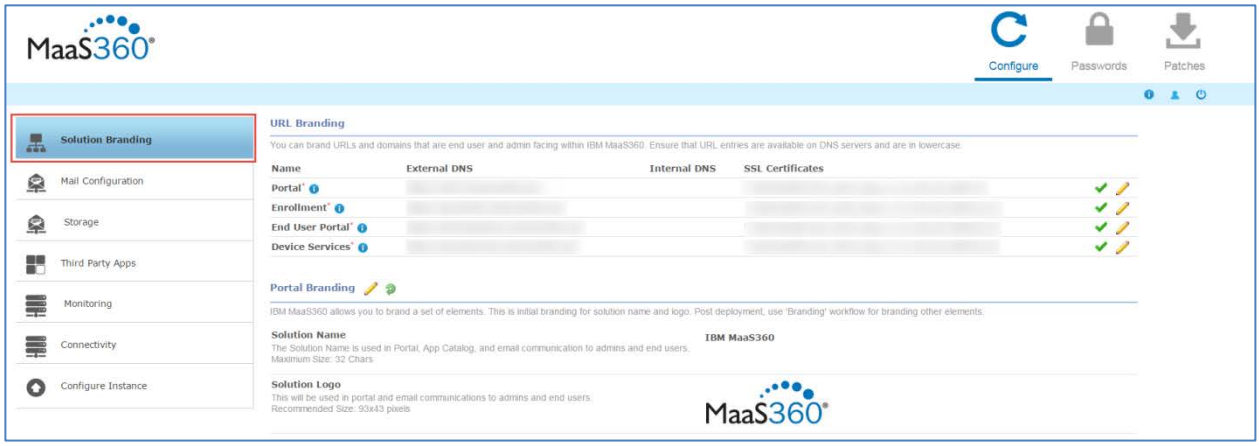
The About screen lets you check component versions:



Solution Branding

Solution Branding is the first tab on the left of the Administration Console.

Here you will indicate the DNS entries for each component host, as well as provide the certificates for these hosts. In addition, your portal can be branded with your company's name and logo.



URL Branding

You can enter the DNS settings and SSL Certificates for each host.

Under the heading URL Branding, click the pencil icon to enter the DNS settings and SSL Certificates for each host. The DNS entries should follow the guidelines in Network Configuration.

External DNS	Enter the External DNS for each component. ***Notes:*** • *For native High Availability deployment without Reverse Proxy, enter the DNS entries configured for external access.* • *For native High Availability deployment with Reverse Proxy, enter the DNS entries configured for external access.* • *For non-native High Availability deployment without Reverse Proxy, enter the DNS entries configured for external access.* • *For non-native High Availability deployment with Reverse Proxy, enter the DNS entries configured for external access.*
Internal DNS	Enter the Internal DNS for each component. ***Notes:*** • *Internal DNS is valid only if Reverse Proxy has been chosen for deployment. In that case, enter the DNS entries configured for internal routing.* • *These URLs are not exposed to the internet and thus provide an added layer of security.* • *Enter http URLs if http traffic is forwarded to MaaS360 VMs or https URLs if https traffic is forwarded to MaaS360 VMs.*

Certificates	Choose whether to upload a new SSL certificate or to use a SSL certificate that you recently uploaded during the configuration of this instance. If you select Use Previous, the only visible field is a drop down list of existing uploaded certificates. The SSL certificates should be issued from a trusted CA. You could use a wildcard certificate for all URLs or separate certificate for each URL. ***Note:*** • For a **Reverse Proxy with HTTPS** deployment you can use self-signed certificates here, although it is recommended to use trusted SSL certificates. However at the Reverse Proxy you should have trusted SSL Certificates.
Use Previous	You can use the certificates of a specific previously configured host by selecting it from the drop down list. A properly configured wildcard certificate can be used for all hosts, for example. This field is only visible if **Use Previous** is selected.
New	If New is chosen then a completely new SSL certificate can be uploaded for the URL.
SSL Certificates	Browse to the SSL certificate to be used for the configuration of this URL. This is either a .crt or .pem file. ***Notes:*** • The SSL certificate file should contain a single domain certificate and should not have intermediate or root certificates in the chain in the file. • You can upload new/renewed certificates after the instance is configured. Make sure you upload renewed certificates and reconfigure the instance before the certificates expire.
SSL Sub CA Certificates	Browse to the certificate authority file. This is either a .crt or .pem file. ***Note:*** • The Sub CA certificate file should contain the issuer Sub CA or a chain in which the issuer Sub CA is present.
Private Key	Browse to the private key for the SSL Certificate for the host. This will be a .key file. The private key must not be password protected. For more information on removing the password, see Appendix D: SSL Certificate Password Removal.

Important:

- After the instance is configured the URLs cannot be changed. A fresh deployment is necessary if URLs have to be changed.

After entering all the information, click **Test** to ensure the settings are configured properly. Errors are reported in red at the top of the screen while a successful test is indicated by a green checkmark. If the test is not successful, check the fields carefully and ensure they match your previous installation settings.

Repeat this process for the **Portal**, **Enrollment**, **End User Portal**, and **Device Services** domains. Use the **Use Previous** radio button to select certificates that were previously entered.

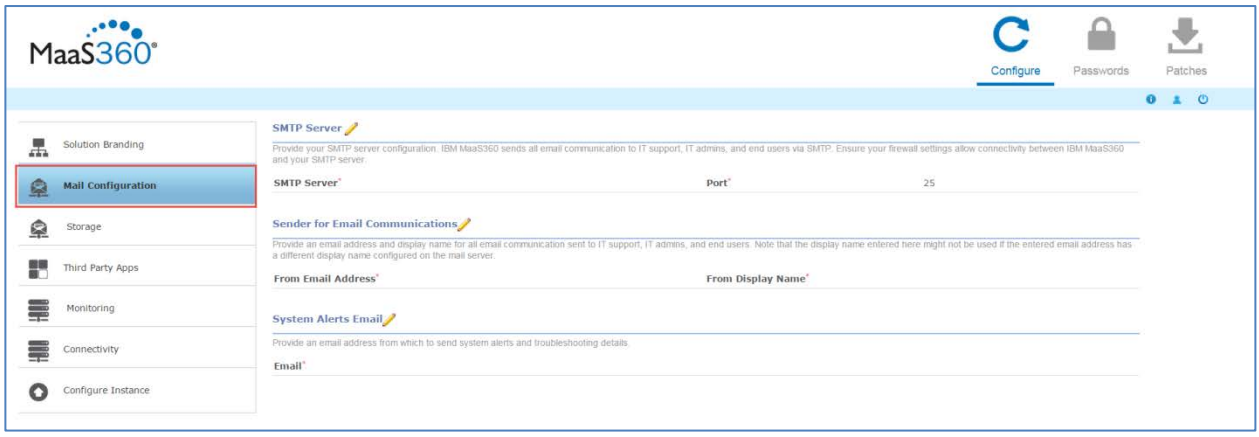
Portal Branding

You can brand the deployment with your name and logo.

Click the pencil icon to see a prompt for a solution name and to upload a logo. The logo should be 93x43 pixels.

Mail Configuration

The **Mail Configuration** tab on the left side of the screen allows you to configure your SMTP server.



SMTP Configuration

Click the pencil icon to edit your SMTP server settings.

SMTP Server	Enter the domain name of your SMTP server. For example, smtp.company.com.
SMTP Port	Enter your SMTP server port. The default value is 25. Click Test to ensure that the settings are configured properly. Errors are reported in red at the top of the screen while a successful test is indicated by a green checkmark. If the test is not successful, check the fields carefully and ensure that they match your deployment.

Sender for Email Communications

Emails that you send to administrators and end users must have an origin.

Click the pencil icon to set the email address and name field for these emails. All emails sent from the IBM MaaS360 deployment will originate from this email address.

This email address must be configured in your SMTP server. The display name set on your SMTP server may override the value entered here.

System Alerts Email

If problems arise with the IBM MaaS360 deployment, the system will send emails to the address entered in the **Systems Alerts** field. In addition, system level emails such as support logs will be sent to this address.

Click the pencil icon to set an administrator email account that will receive these messages.

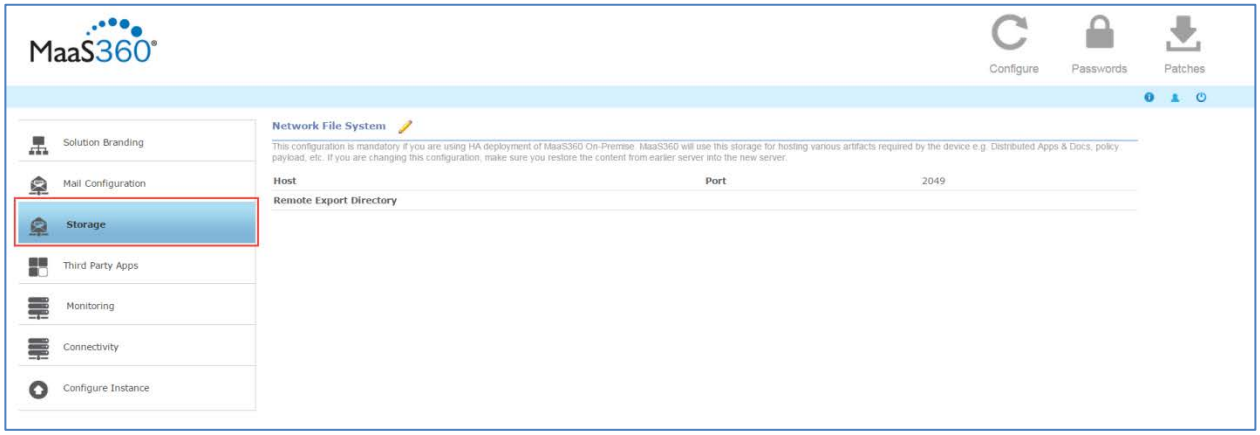
Storage

The Storage tab allows for configuring storage in an external Network File System (NFS) server, a shared storage for CDN content including applications, documents and MaaS360 Agent Application artifacts.

Click the pencil icon to edit the information.

Notes:

- Storage is mandatory for a native High Availability deployment.
- Check the requirements for the Network File System (NFS) Server.
- This step is optional for non–native High Availability deployment.
- This is an irreversible configuration for the life of the instance.



Host	Enter the hostname or IP Address of the remote NFS server. Ensure the host is reachable from the Services and Standalone VMs of the MaaS360 vApp.
Port	Enter the port number of the NFS server. The default value is 2049.
Remote Export Directory	Enter the remote directory in the NFS server that will be exported as CDN storage space for MaaS360.

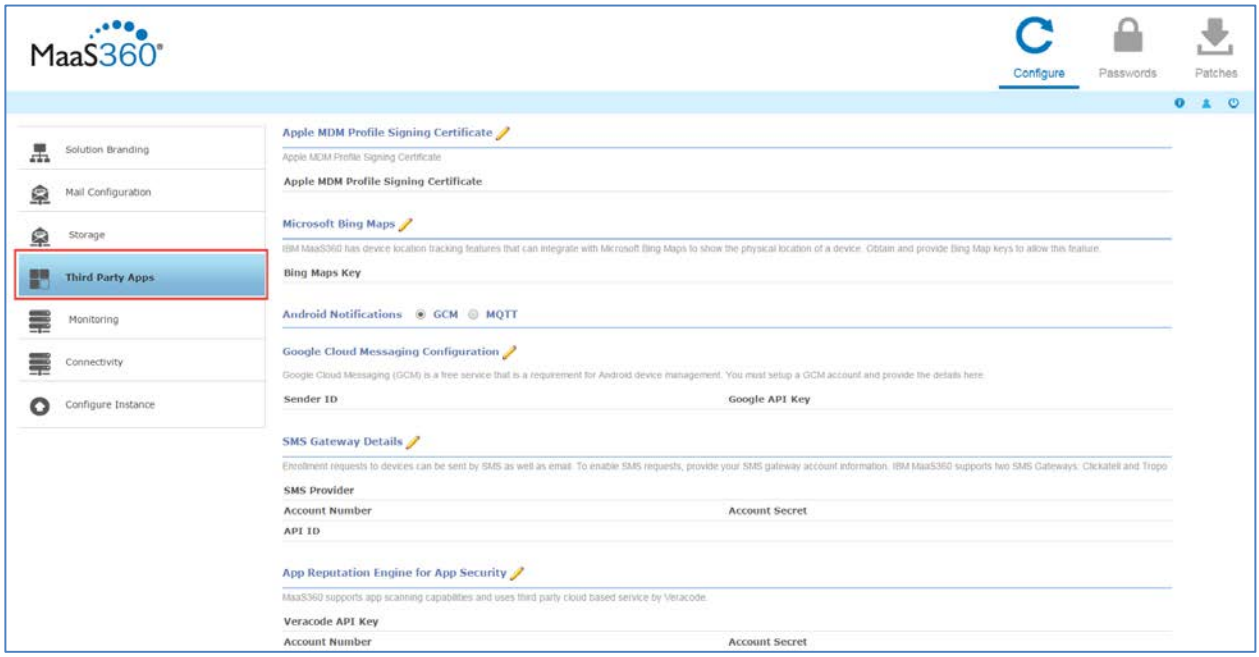
Notes:

- If the NFS server or the export directory is not accessible from MaaS360 you will lose the content that gets uploaded into MaaS360.
- Ensure high availability of the NFS server to avoid data loss.

- The export directory contents should be backed up frequently to minimize data loss if there is a hardware or software failure.
- Ensure you have a defined procedure to restore the backed up data into the NFS server.

Third-Party Applications

The **Third Party Apps** tab allows the configuration of several features that use third-party systems to enhance IBM MaaS360.



Apple MDM Profile Signing Certificate

Apple profile signing certificate is a code signing certificate used to sign the MDM profile that gets installed on Apple devices.

Click the pencil icon  to make your changes.

You can use the existing SSL certificate uploaded with the Services URL in the URL branding section or obtain a code signing certificate and upload it.

You can also upload a new signing certificate. Choose an SSL Certificate, SSL SubCA Certificate or Private Key.

Note: *For Reverse Proxy deployment with http traffic routed to MaaS360 you have to upload a certificate with the* Upload New *option. This could be either a code signing certificate or a SSL certificate. Make sure the certificate uses 2048-bit keys.*

Click **Save**.

Microsoft Bing Maps

IBM MaaS360 has device location tracking features that can integrate with Microsoft Bing Maps to show the physical location of a device. If you want to implement those features, you need a Bing Maps Key.

Click the pencil icon .

Enter the key and click **Save**.

Android Notifications

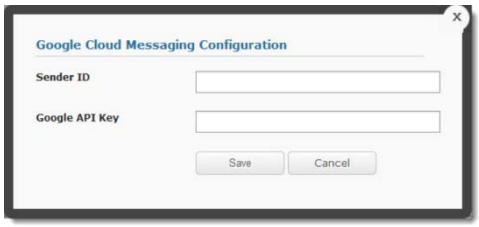
Two communication protocols are available to facilitate Android communication.

You must configure the communication protocols GCM or MQTT to allow communication with Android devices.

Choose the GCM or MQTT radio button and click the pencil icon .

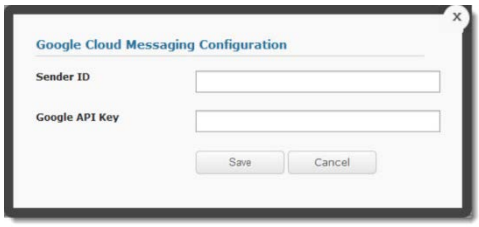
Setting up a Google Cloud Messaging Configuration

Choose **GCM** and click the pencil icon .



Google Cloud Messaging (GCM) is the primary protocol for Android communication. You must set up a free GCM account and provide the **Sender ID** and **Google API Key**. For more information about GCM, see http://developer.android.com/google/gcm/gs.html.

Note: *The* Sender ID *is also referred to as the* Project Number*. The* Sender ID *is not the email address associated with your GCM account.*



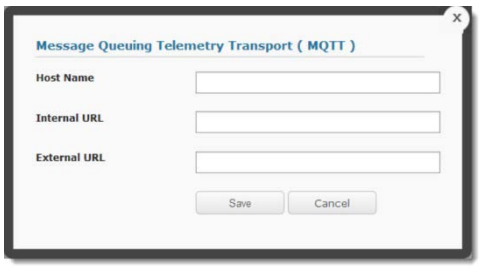
Click **Save**.

Setting up Message Queuing Telemetry Transport (MQTT)

Choose the **MQTT** radio button and click the pencil icon .

MQTT is an optional protocol that is used for Android communication. It is necessary for integration with IBM® MessageSight™ product. To configure MQTT, enter the appropriate hostname, internal, and external URLs. Edit and update the default values with valid values.

Note: *Refer to the* IBM MessageSight Configuration for MaaS360 *guide for information about configuring a MessageSight server for MaaS360 Android notifications.*



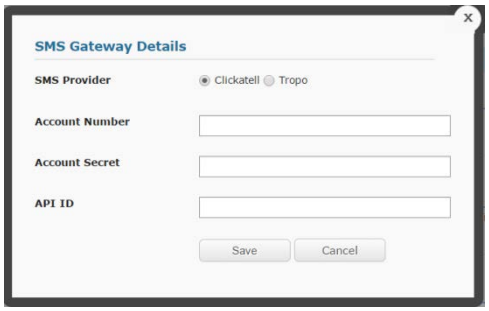
Click **Save**.

SMS Gateway Details

Device enrollment requests can be issued by email or SMS.

To enable SMS requests, you must set up an SMS Gateway account with a third-party provider. This is an optional feature. Currently, two SMS providers are supported, Clickatell and Tropo.

Enter the **Account Number**, **Account Secret** and **API ID** provided by your SMS provider.



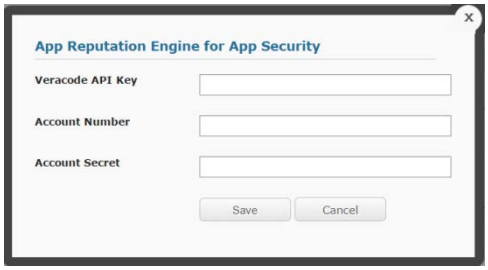
Click **Save**.

Application Reputation Engine for Application Security

MaaS360 provides a way to integrate with an external Application reputation provider, Veracode. This is an optional feature.

Use it to get the latest ratings for Android Applications hosted in Google Play Store.

Get the **Veracode API Key**, **Account Number** and **Account Secret** from Veracode, and then enter them.



Click **Save**.

Note: *For Veracode license key verification to be successful, outgoing access to the internet should be available. If you notice any errors related to failure in verification, make sure the Portal VMs have outgoing access to internet. This verification is performed in MaaS360 Portal in the Application Management workflow.*

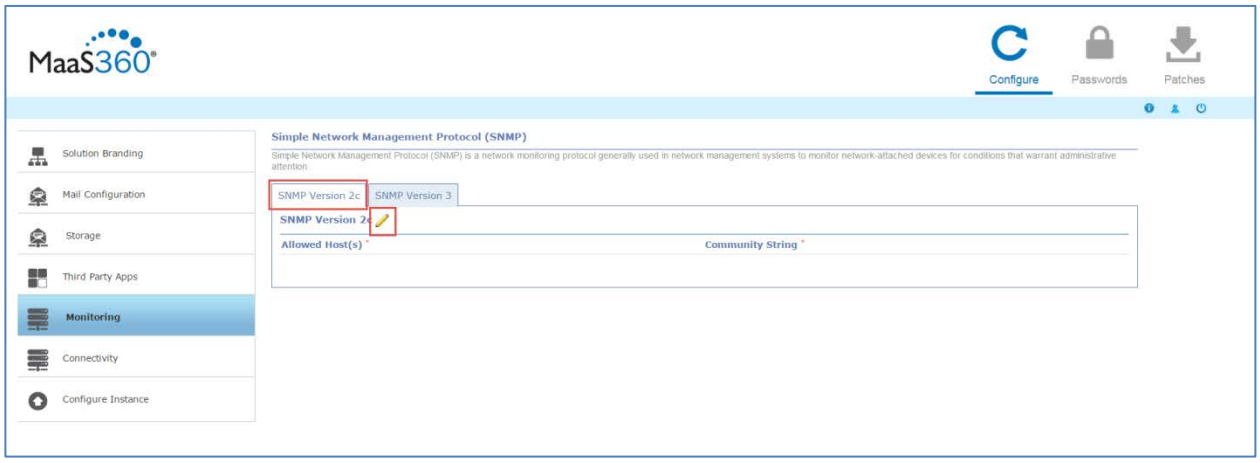
Monitoring

The **Monitoring** tab allows the configuration of the Simple Network Management Protocol (SNMP). Using SNMP is optional.

IBM MaaS360 supports SNMP v2c and v3.

Select the appropriate tab and click the pencil icon  to configure SNMP.

SNMP Version 2c (v2c)

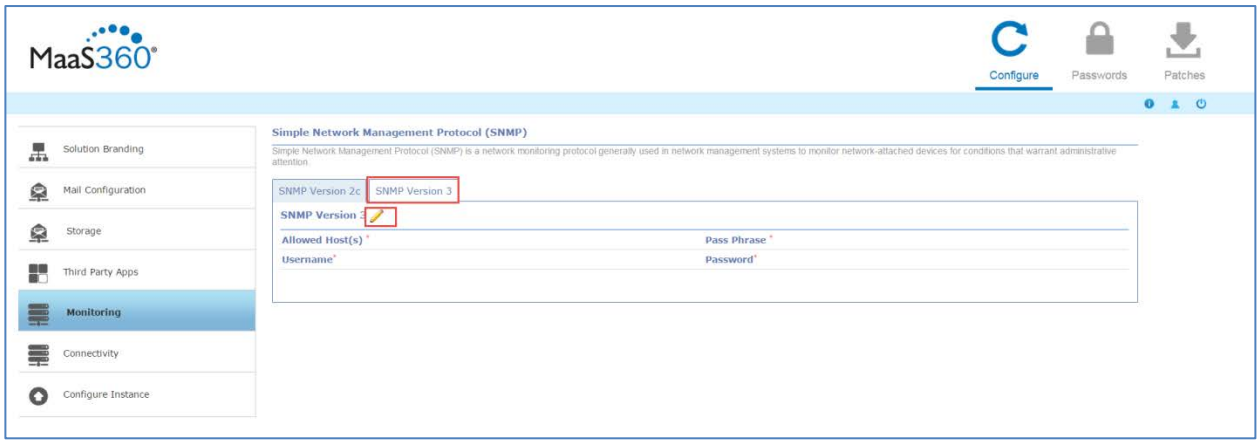


For the **Allowed Host(s)**, enter a comma separated list of IP addresses or hostnames for those hosts that are authorized to monitor the seven IBM MaaS360 VMs.

Enter the Community String.

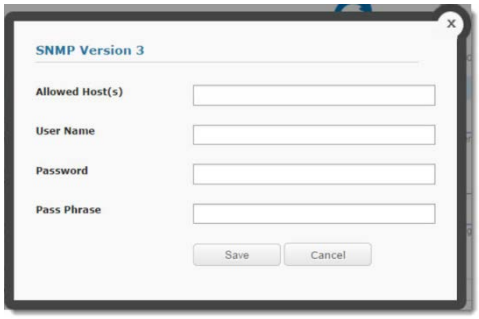
Click **Save**.

SNMP v3



Under **Allowed Host(s)**, enter a comma delimitated list of IP addresses or hostnames for those hosts that are authorized to monitor the seven IBM MaaS360 VMs.

Enter the appropriate **User Name**, **Password**, and **Pass Phrase**.



Click **Save**.

MaaS360 Application Monitoring

SNMP clients can be used to monitor the MaaS360 modules hosted in the seven MaaS360 VMs.

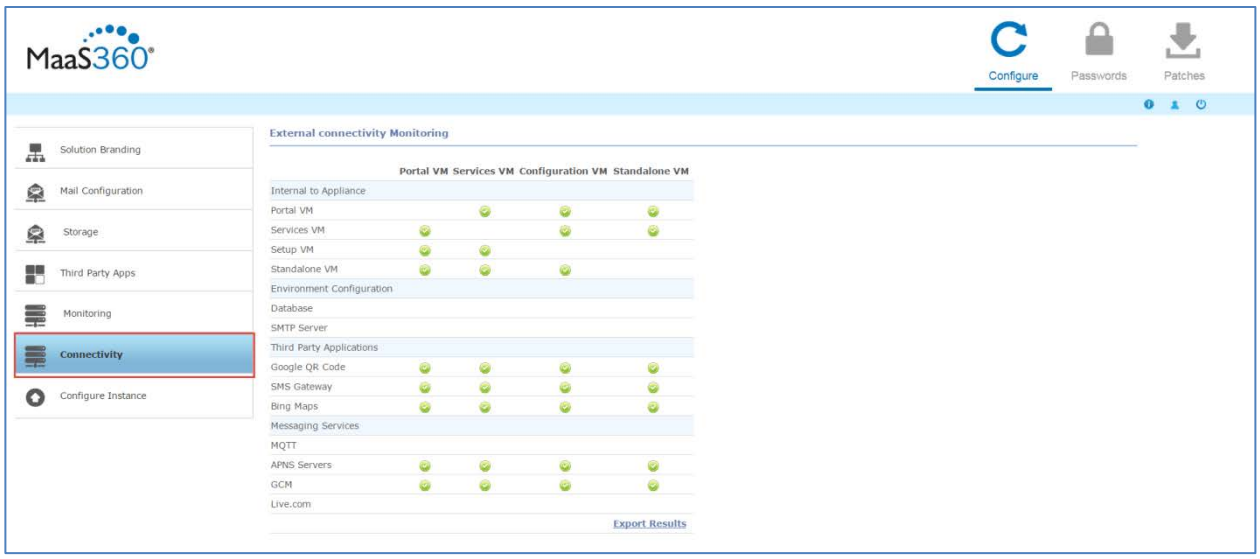
OIDs or Object Identifiers are assigned to various MaaS360 module level attributes representing Memory, Database Connections, Application State, CPU usage, Open Files, Uptime & Thread Count. These OIDs can be monitored through SNMP.

The list of available OIDs can be accessed at https://<Configuration_VM>:8443/static/MaaS360-OIDs.txt

This URL provides OID list for 1-0 virtual machines. The same set of OIDs work for 1-1 virtual machines of the same type.

Connectivity

On the **Connectivity** tab you can see the network connectivity of the MaaS360 VMs with external systems, Database, and within themselves. All port connections should show up as green checkmarks before you continue with the configuration of the instance.



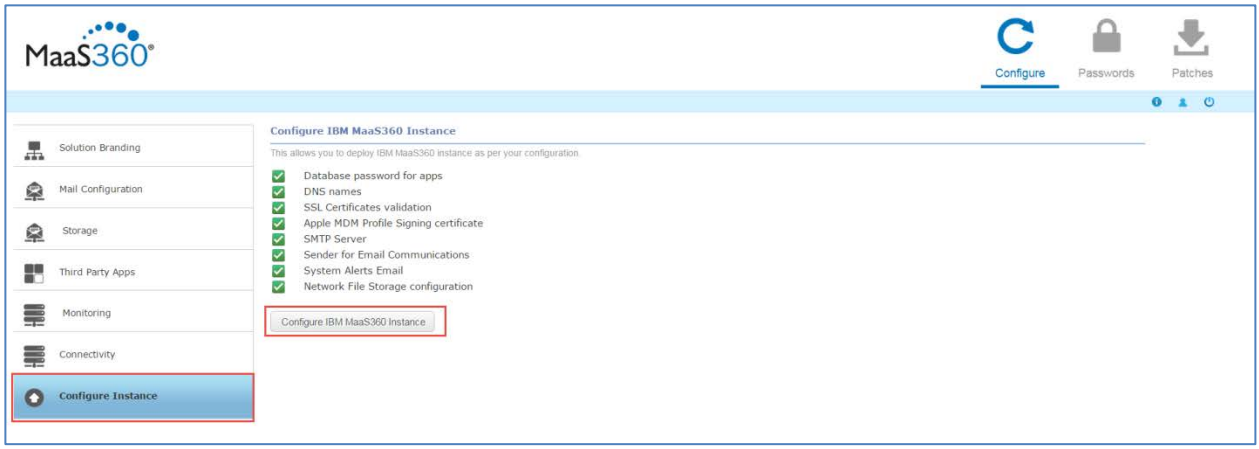
Important:

- If you see a red X, hover over it to see the error message. Take the appropriate actions to fix the reported errors, refresh the page and see if the errors are gone. Make sure all errors are resolved before you proceed further with the configuration.
- Configuring the instance with pending errors may result in configuration failure or loss of functionality.

Configure Instance

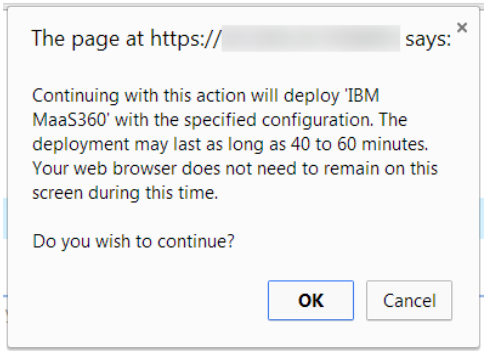
After all settings are configured, click the **Configure Instance** tab. This tab verifies that all settings are properly configured.

Check each entry and ensure that a green checkmark is displayed next to each item. If any item is not configured properly, return to the appropriate location and correct the setting.



After you ensure that all settings are in compliance, select **Configure IBM MaaS360 Instance** to transfer your configured settings to the database.

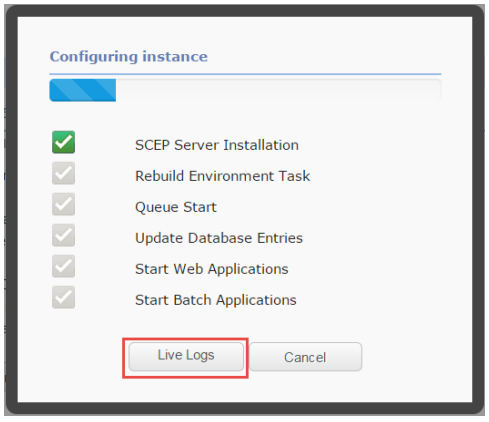
A confirmation window will appear. Select **OK** to continue.



A progress bar displays the configuration status. It takes several minutes before any progress is reflected, and the entire process can take up to an hour.

A static snapshot of the configuration log can be accessed by selecting **Live Logs**. Use this feature to ensure that configuration is progressing.

Configuration continues even if the browser window is closed. If you exit your browser, you can log back in to the Administration Console and select the **Configure Instance** tab again to view the progress.



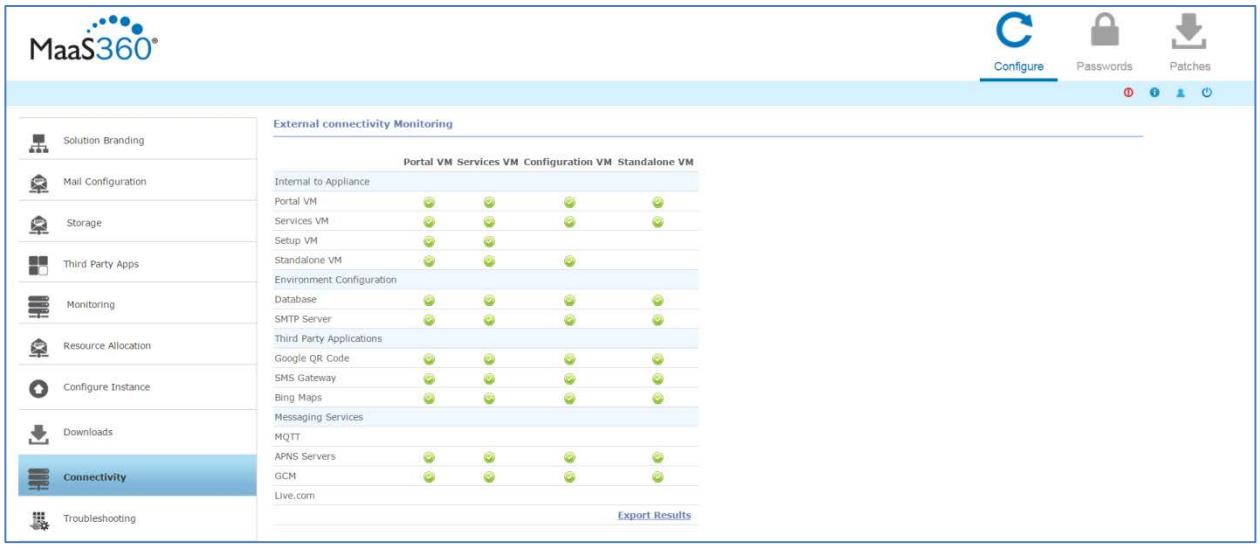
Note: *After the configuration has completed, it is a best practice to look at the* ***Connectivity*** *and* ***Troubleshooting*** *tabs on the left side of the screen to review the overall health of the system and fix any errors that have been reported.*

Connectivity

After the instance has been successfully configured, check the network connectivity between the MaaS360 VMs and external system, the database and themselves. All port connections should have a green checkmark before you continue.

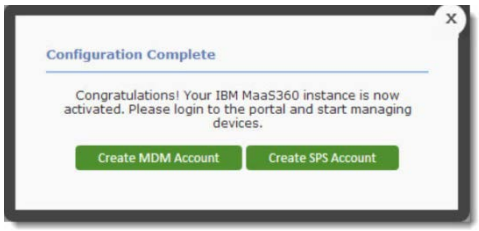
Important:

- If you see a red X, hover over it to see the error message. Take the appropriate actions to fix the reported errors, refresh the page and see if the errors are gone. Make sure all errors are resolved before you proceed further with the configuration.
- Configuring the instance with pending errors may result in configuration failure or loss of functionality.



Account Configuration

When configuration completes, you are prompted to create an account.



Click either **Create MDM Account** or **Create SPS Account** to create the specified account type. A new tab opens to the associated account creation portal. For more information about creating an account, see *IBM MaaS360 Mobile Device Management Configuration Guide*.

Close this window to return to the Administration Console if you do not want to create an account at this time.

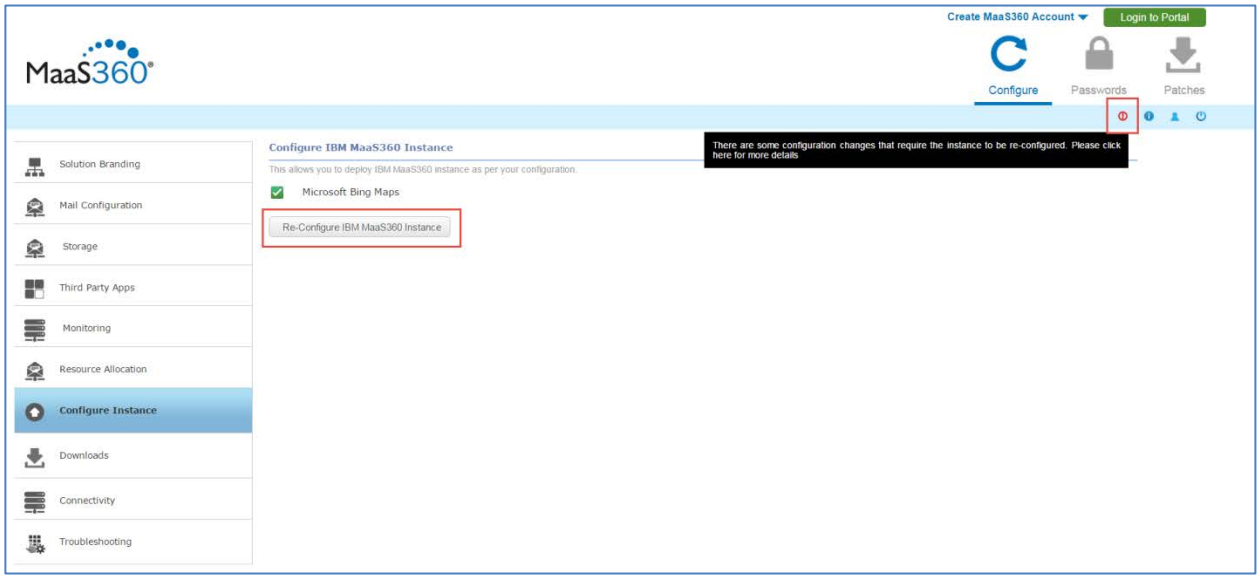
You can also create accounts from a menu at the top right corner of the Administration Console.

Reconfigure

After configuration is complete, you can change settings to reconfigure your deployment.

After you configure your deployment, the **Configure Instance** tab displays a **Re-Configure IBM MaaS360 Instance** button. This button is available only if a setting is changed. Any settings that have been changed since you last configured, are listed above the button. You can review any them and click **Re-Configure IBM MaaS360 Instance** to deploy the changes.

Any time a change is made in the Administration Console, a red icon displays near the **About**, **User**, and **Logout** buttons. If you hover over it, you will receive a message that changes were made that are not yet deployed.

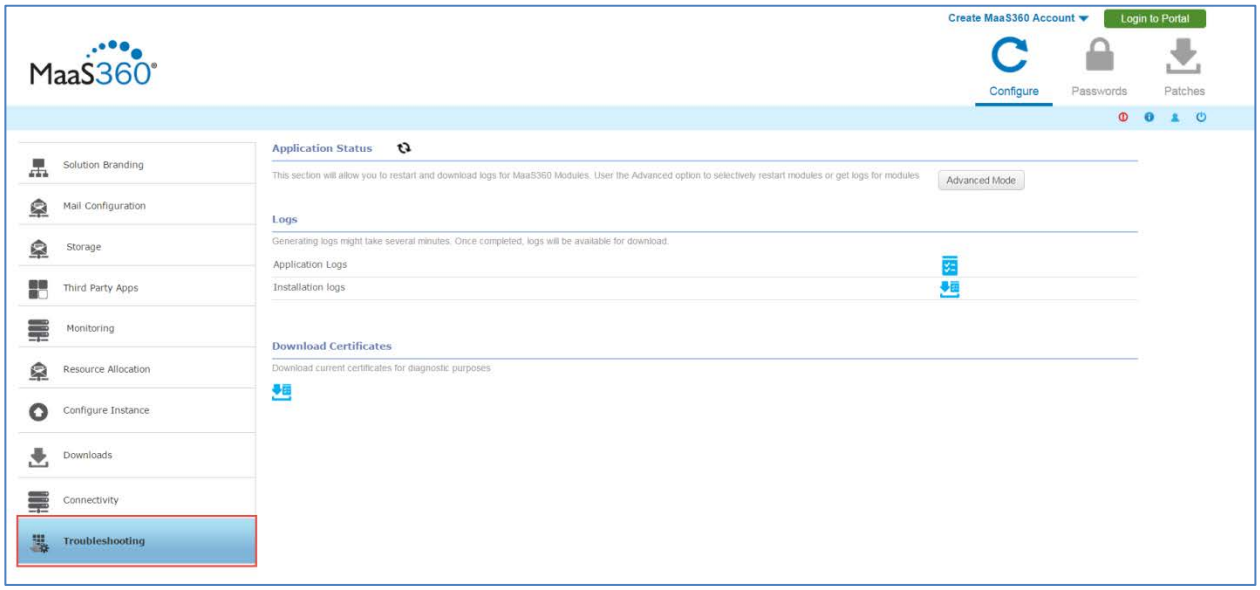


Important:

- Any changes that are made in the Administration Console are not deployed instantly. Instead, you must reconfigure the instance using **Re-Configure IBM MaaS360 Instance**.
- The process takes several minutes to complete. As with the initial configuration, a snapshot of the logs can be viewed to verify that the process is active.
- After configuration completes, the system requires a 10-minute waiting period before access to the Administration Console is granted. This is reflected in the live logs.
- After a reconfiguration, it is a best practice to look at the **Connectivity** and **Troubleshooting** tabs on the left side of the screen to review the overall health of the system and fix any errors that have been reported.

Troubleshooting

The **Troubleshooting** tab is available after you have configured your instance. It provides an overall view of the health of your IBM MaaS360 deployment.

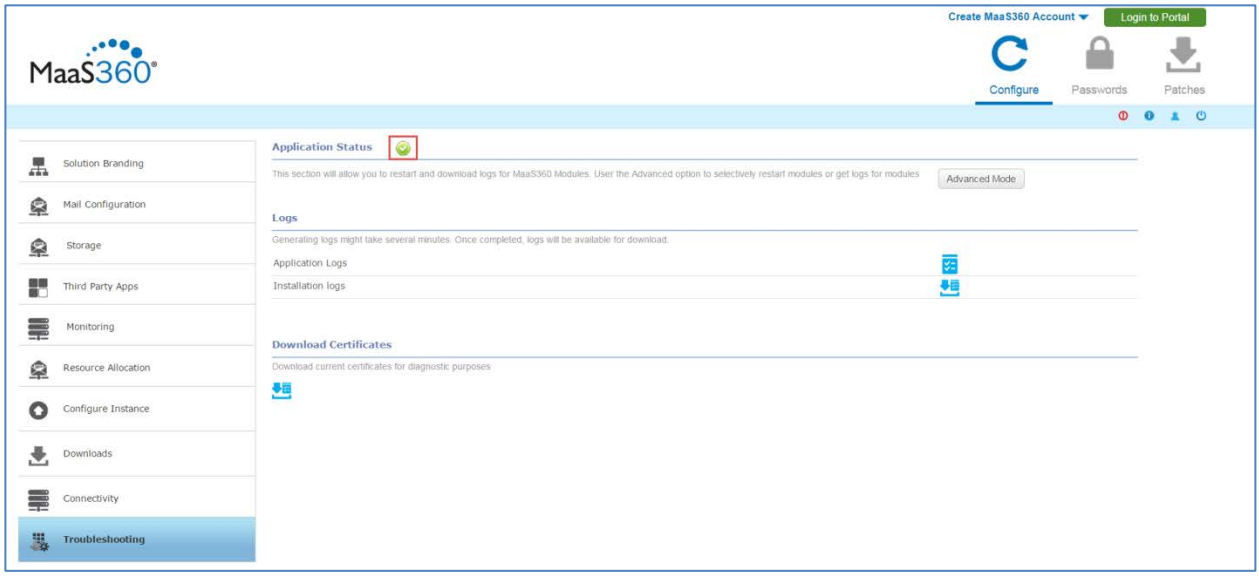


Application Status

You can validate all applications that are part of your IBM MaaS360 instance.

When you access the **Troubleshooting** tab, the Administration Console conducts a health check of all web and batch applications that are part of your IBM MaaS360 deployment. This query is indicated by a spinning arrow icon. After the health check completes, a green check mark icon is displayed showing that no problems were found. If any applications fail the health test, they are listed.

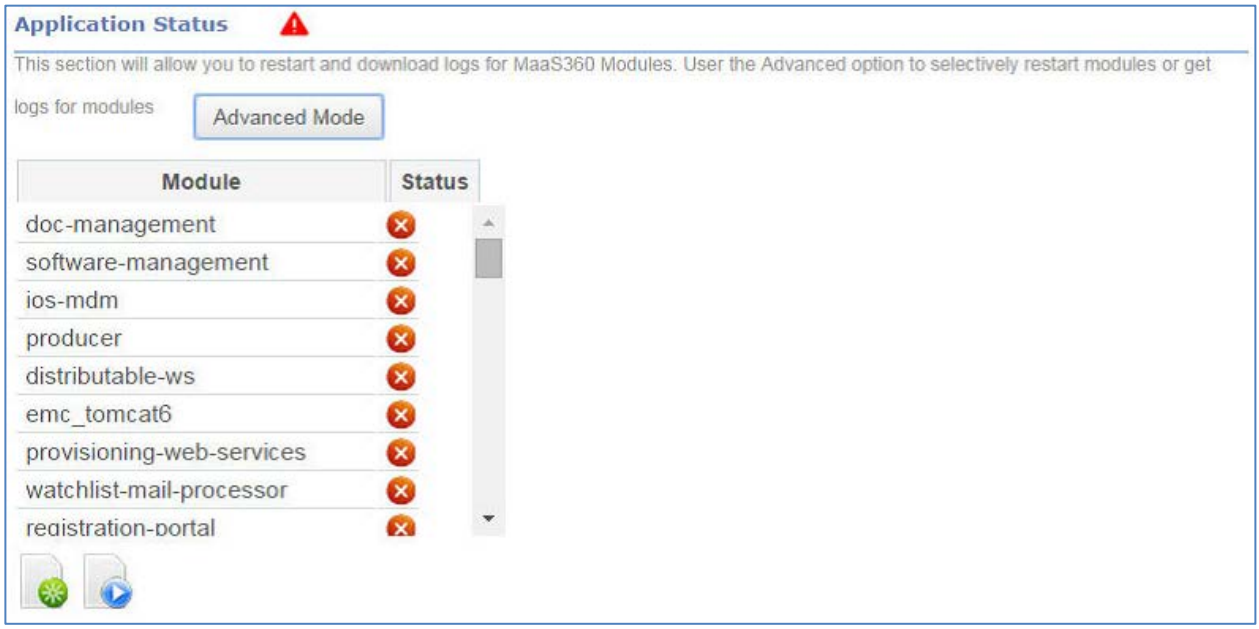
Failed applications can be handled as a group, or they can be interacted with individually in an advanced mode.



Basic Mode

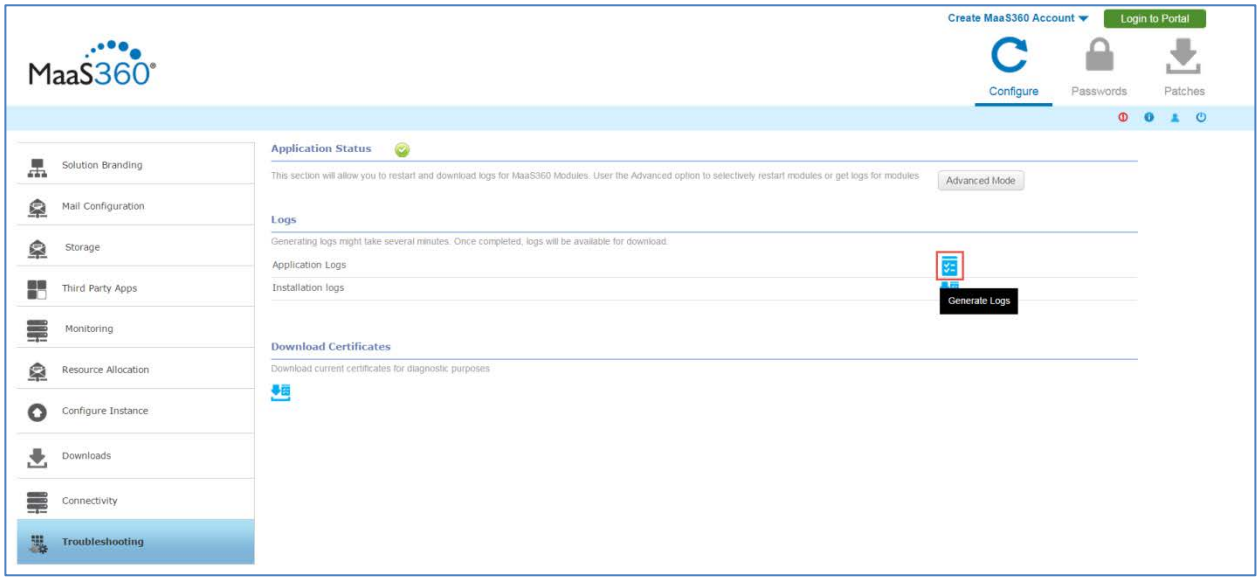
Failed applications can be handled as a group when troubleshooting in basic mode:

1. Generate the log files for the failed applications using the associated button. This step may take several minutes.
2. Use the link provided to download the generated logs and preserve them.
3. Restart the failed applications using the associated button. This process will take several minutes. If necessary, navigate to a different tab and return to the **Troubleshooting** tab to query the applications again.
4. If applications continue to fail, generate the logs for the failed applications again, and preserve them.
5. Contact IBM Software Support.



Collect Application Logs

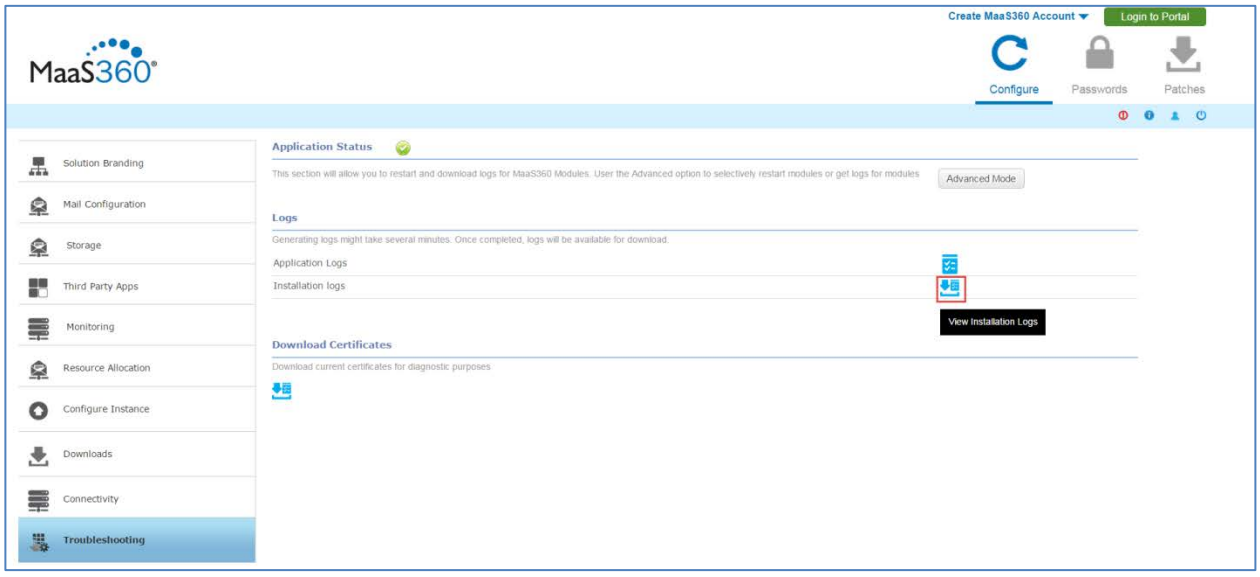
Click **Generate Logs** to generate the logs.



A pop-up box provides the download link.

View Installation Logs

Click **View Installation Logs** to see them in a separate browser window.

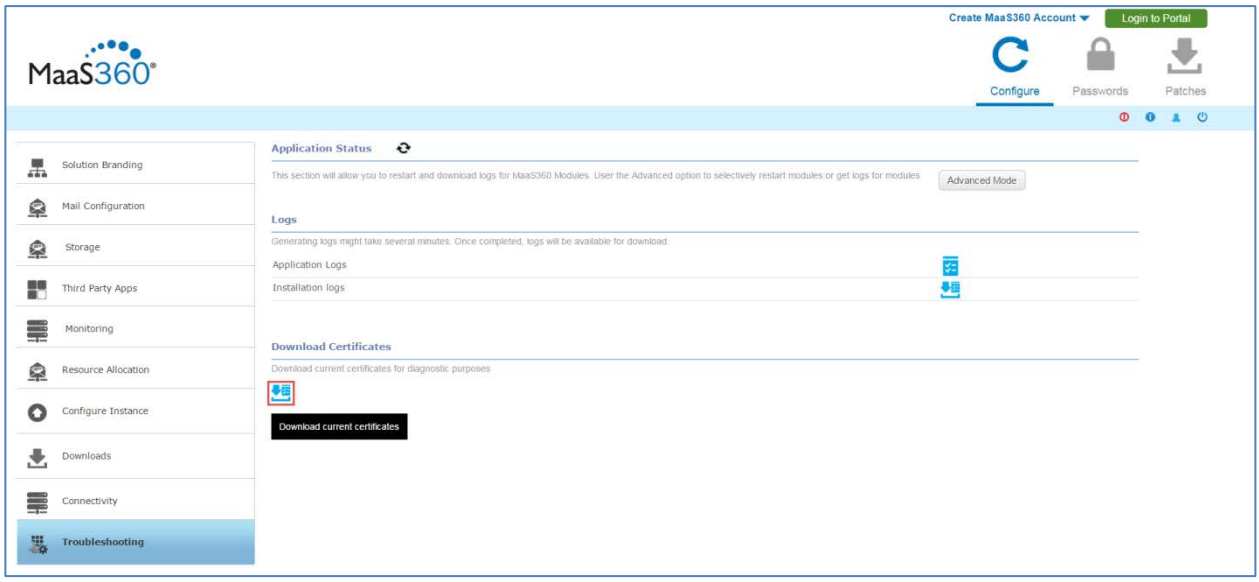


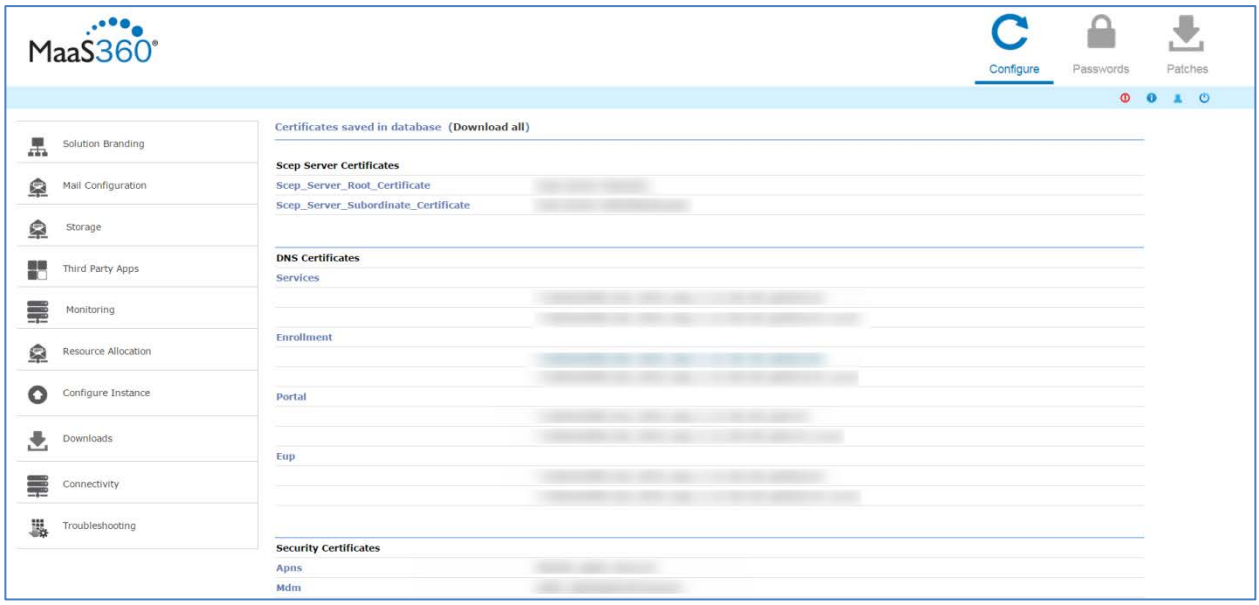
Download Certificates

All of the certificates that are used to configure your IBM MaaS360 deployment can be downloaded for reference.

The ability to download the currently deployed certificates can be used to help determine whether the correct certificates were used. A new browser window is opened that provides links to each certificate saved in the database.

Note: *Private Key files for certificates cannot be downloaded for security reasons.*

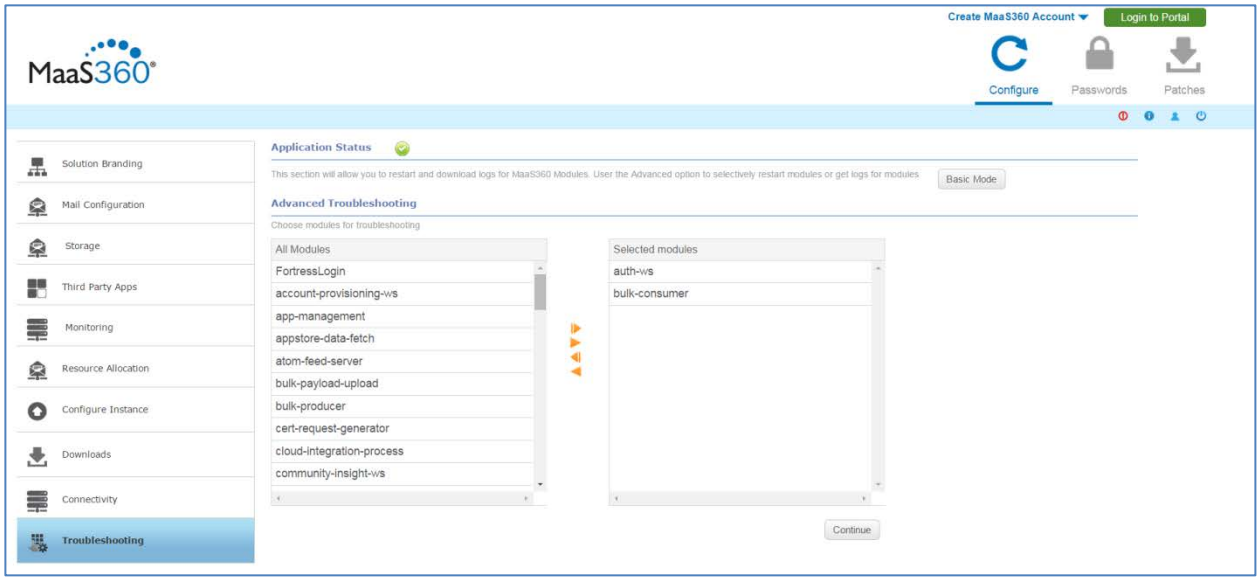




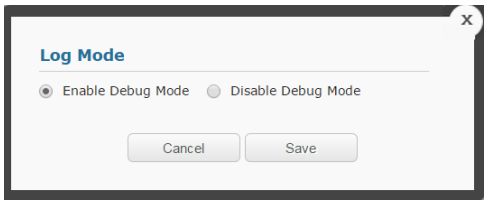
Advanced Mode

Troubleshooting in Advanced mode allows interaction with individual failed applications:

1. Select the applications that you want to troubleshoot with the arrow icons and click **Continue**.

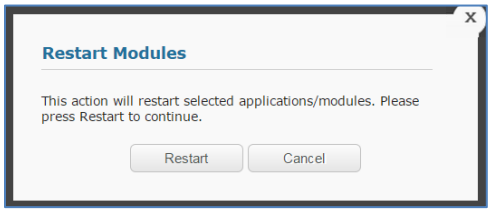


2. After the console queries the applications, select the appropriate applications by selecting the checkmark. All listed applications can be selected with the master checkbox at the top of the list.
3. Click the **Change Log Mode** button and save your preference to enter or exit Debug mode.

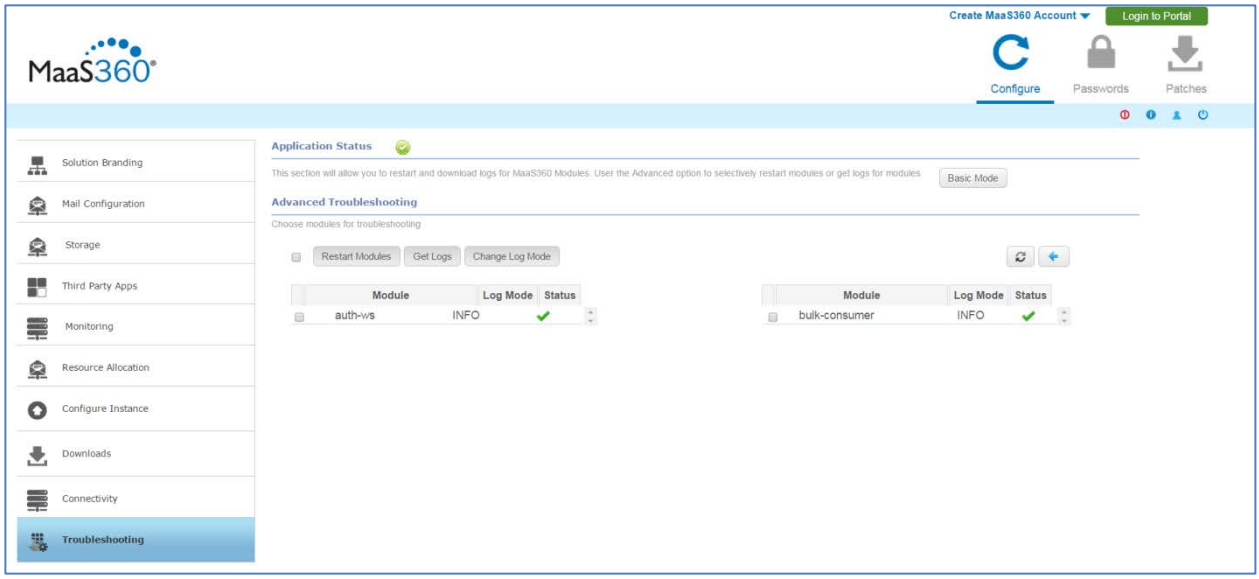


4. Click **Get Logs** to generate the log files for the selected applications. You will be prompted to download them. Save them for future reference.

5. Click **Restart Modules** to restart the selected applications.

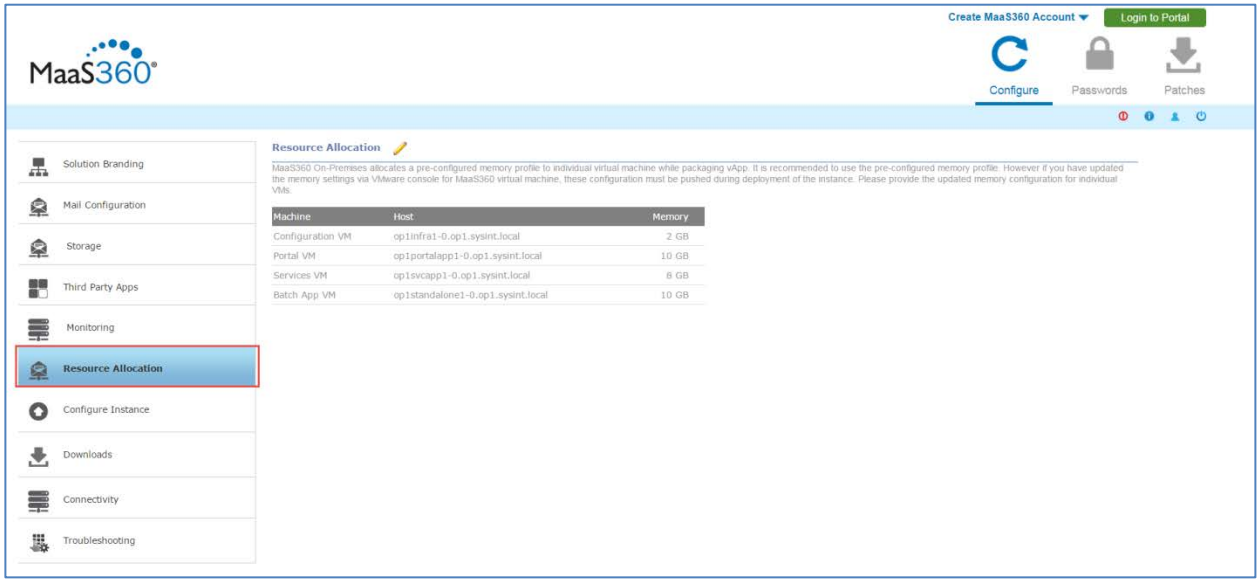


6. The refresh button  manually queries the applications to update their status. The blue back button  can be used to go back a screen to select different applications.
7. If applications continue to fail, contact IBM Software Support and be prepared to provide the downloaded log files.


Create MaaS360 Account
Login to Portal
MaaS360
Configure
Passwords
Patches
Solution Branding
Mail Configuration
Storage
Third Party Apps
Monitoring
Resource Allocation
Configure Instance
Downloads
Connectivity
Troubleshooting
Application Status
This section will allow you to restart and download logs for MaaS360 Modules. User the Advanced option to selectively restart modules or get logs for modules
Basic Mode
Advanced Troubleshooting
Choose modules for troubleshooting
Restart Modules
Get Logs
Change Log Mode
Module
Log Mode
Status
auth-ws
INFO
Module
Log Mode
Status
bulk-consumer
INFO

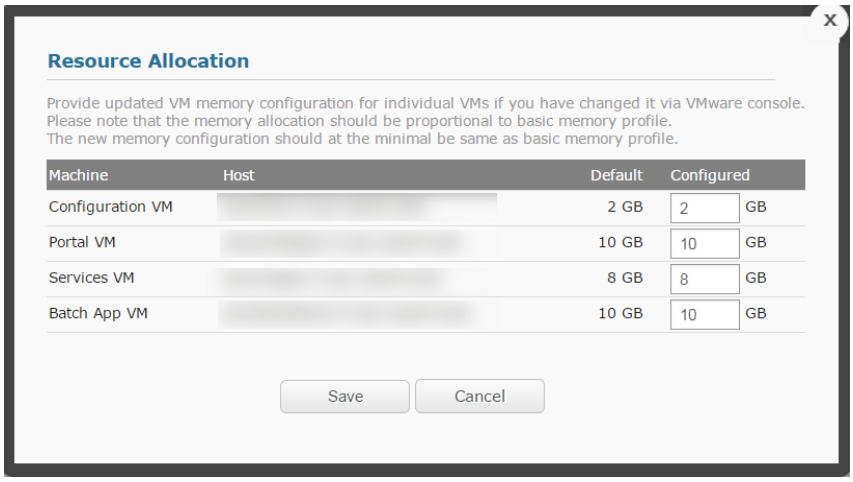
Resource Allocation

The **Resource Allocation** tab allows the configuration of memory allocated to the applications running in the MaaS360 VMs. For increased scalability you have to allocate extra memory in addition to the predefined memory configuration of MaaS360 VMs.



Enter the updated VM memory value in the **Configured** field and click **Save**.

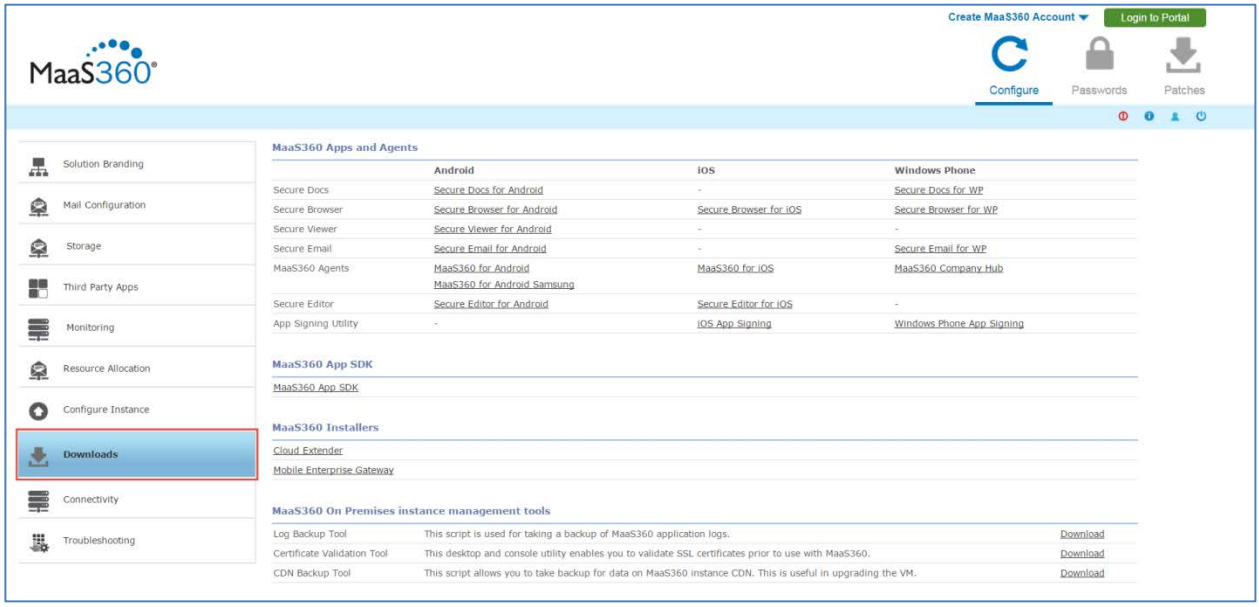
You cannot enter values less than the default values.



Note: *Make sure you have already increased the memory of all VMs through VMware vCenter and then enter the new VM memory values here. The increase in memory for Portal, Services and Standalone VM pairs should be the same.*

Downloads

After configuration, the **Downloads** tab is available in the Administration Console. It provides an interface where various apps and utilities are downloaded to support your deployment. Many of these downloads are discussed in more detail in the *IBM MaaS360 Mobile Device Management Configuration Guide*.



MaaS360 Apps and Agents

The **Apps and Agents** portion of the **Downloads** tab provides links to various agents and utilities. Several agents for iOS, Android, and Windows Phone are available to download. In addition, the App Signing Utilities for iOS and Windows Phone are available.

Note: *Android apps do not require app signing.*

The process of code-signing iOS and Android apps is discussed in detail in the *IBM MaaS360 Mobile Device Management Configuration Guide*.

The following apps and utilities are available:

- Android
  - MaaS360 for Android
  - MaaS360 for Android Samsung
  - Secure Docs for Android
  - Secure Browser for Android
  - Secure Viewer for Android
  - Secure Email for Android
  - Secure Editor for Android
- iOS
  - MaaS360 for iOS
  - Secure Browser for iOS
  - Secure Editor for iOS
  - iOS App Signing

- Windows Phone
  - MaaS360 Company Hub
  - Secure Docs for WP
  - Secure Browser for WP
  - Secure Email for WP
  - Windows Phone App Signing

MaaS360 App SDK

Applications SDKs for iOS and Android that can be integrated with enterprise apps are available. Details can be found in the *IBM MaaS360 Mobile Device Management Configuration Guide*.

MaaS360 Installers

The **Downloads** tab provides links to two important installers.

1. The IBM MaaS360 Cloud Extender is a program that functions as a bidirectional communication portal that allows your deployment to communicate with third-party platforms such as Exchange Server. For more information, see the *IBM MaaS360 Cloud Extender Guide*.
2. The IBM MaaS360 Mobile Enterprise Gateway is a utility that allows behind-the-firewall access to your deployment without the need to change your network or firewall configuration. One or both of these utilities might be required depending on your deployment and the devices that are managed. For more information, see the *IBM MaaS360 Mobile Enterprise Gateway Guide*.

MaaS360 Management Tools

The **Downloads** tab provides links to several management tools that are available to help manage your IBM MaaS360 deployment:

Log Backup Tool

This utility backs up log files.

Certificate Validation Tool

This utility allows the creation and verification of SSL certificates before deployment in your instance.

CDN Backup Tool

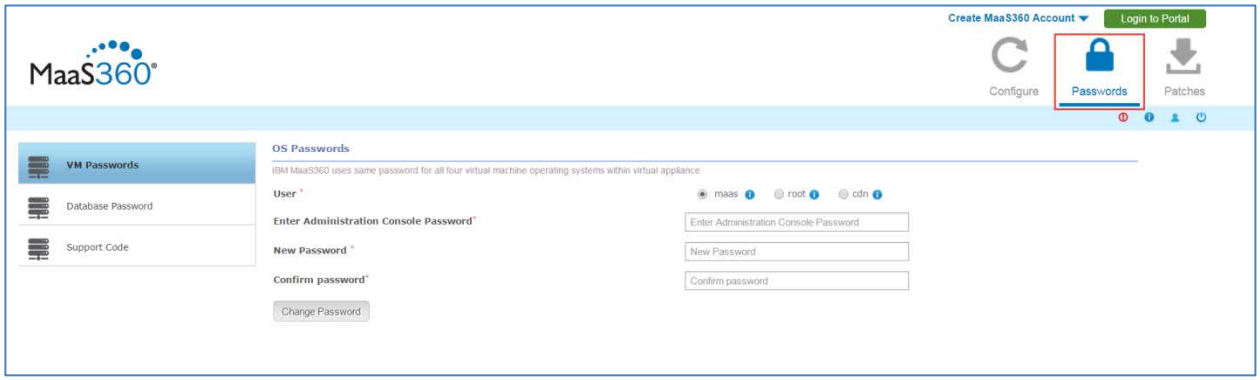
This utility allows the manual backup of the Content Delivery Network (CDN) content. The CDN content can be backed up separately from the Services VM backup that is part of the standard backup protocol. For more information, see CDN Backup.

Passwords

VM Passwords

Click the **Passwords** icon in the upper-right corner of the screen to manage the passwords for the operating systems of each virtual machine.

All seven of the virtual machines that are contained in the virtual appliance share the operating system password.



There are three user accounts:

1. The **root** user cannot log in remotely.
2. The **maas** user can log in remotely and can gain access to the root. For more information about accessing root remotely, see Appendix C: VM Root Log In.
3. The **cdn** user is used to back up the Content Delivery Network on the Services VM. For more information about backing up the CDN, see CDN Backup.

Select the user whose password you want to change. Enter the new password, and click **Change Password** to update each virtual machine. You must enter your current Administration Console password as a security measure.

The default password for the root, maas, and cdn users is **MaaS360_Console**.

The operating system passwords can be changed at any time without the need to reconfigure the entire deployment.

Database Password

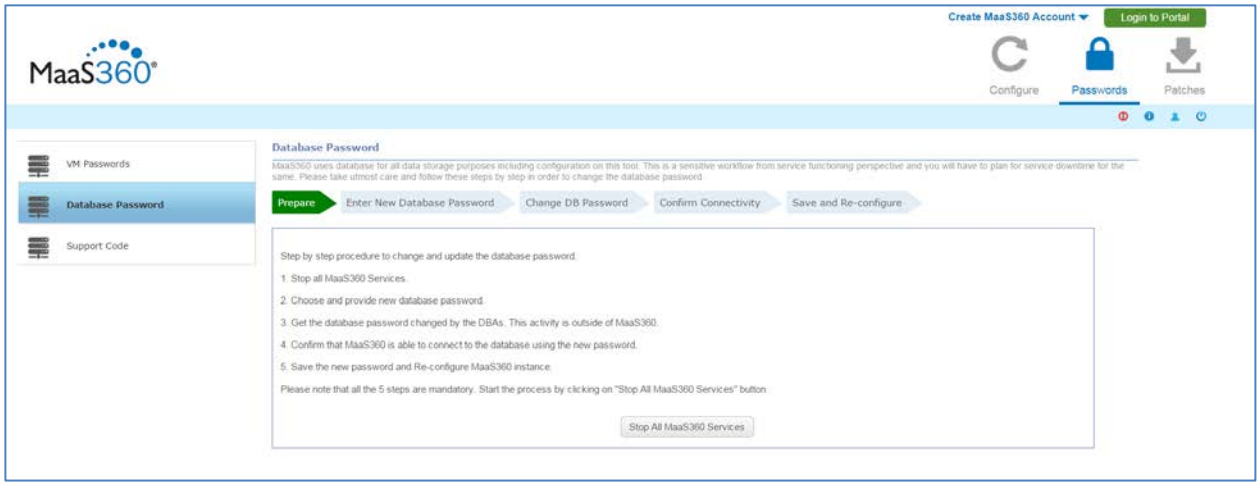
The **Database Password** wizard guides you to update the password required when connecting to MaaS360 databases from MaaS360 vApp.

Note: *This workflow should be used whenever there is a need to update the database password. Ensure you execute this workflow before the existing database password expires.*

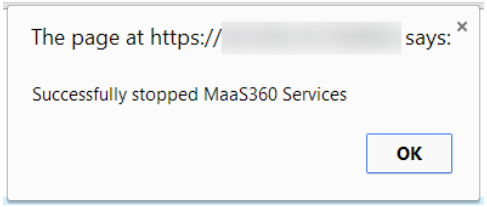
Important

This is a critical workflow and should be performed carefully. Note that it has downtime implications. Plan for the downtime before executing this workflow.

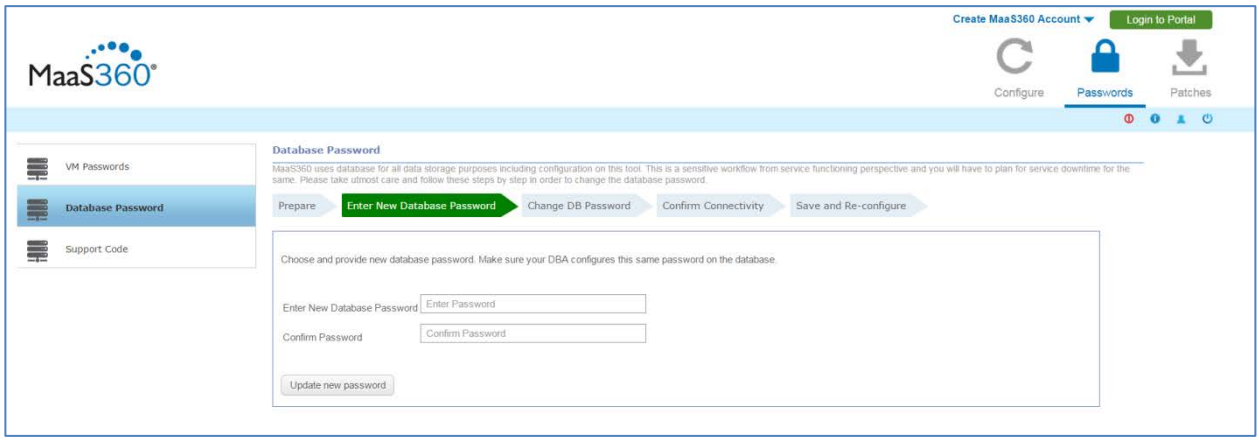
The list of steps to be executed in this wizard is listed in **Prepare**. Make sure you review the steps and understand clearly what needs to be done.



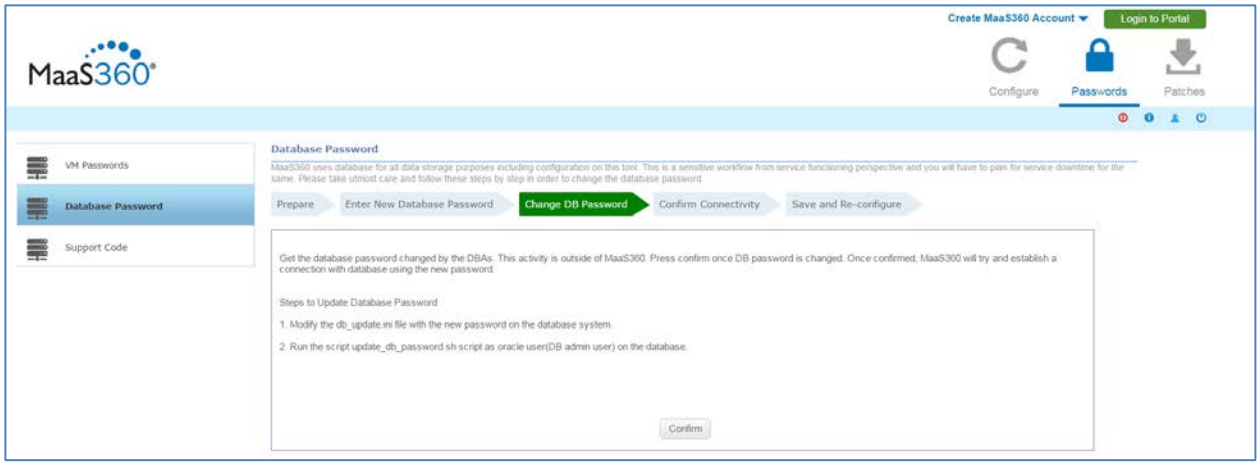
1. Click **Stop All MaaS60 Services** to shut down all applications inside the vApp. This step will take a while to complete. Please do not refresh the page till the process completes and you see the following response:



2. Click **OK** to continue.
3. Enter the new database password and click **Update new password**.

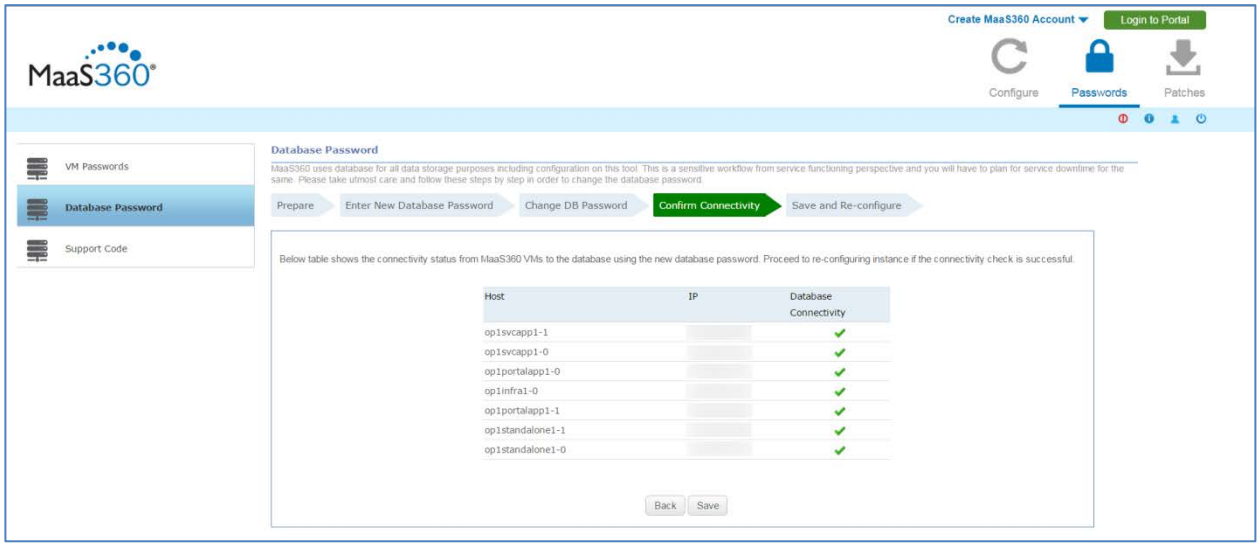


4. The next step must be performed outside of the MaaS360 Administrative Console. Follow the steps outlined in this page to change the password for MaaS360 databases. The files mentioned below are part of the database artifact. The script has to be executed on Oracle server.
5. After the password has been successfully changed at the database level click **Confirm.**



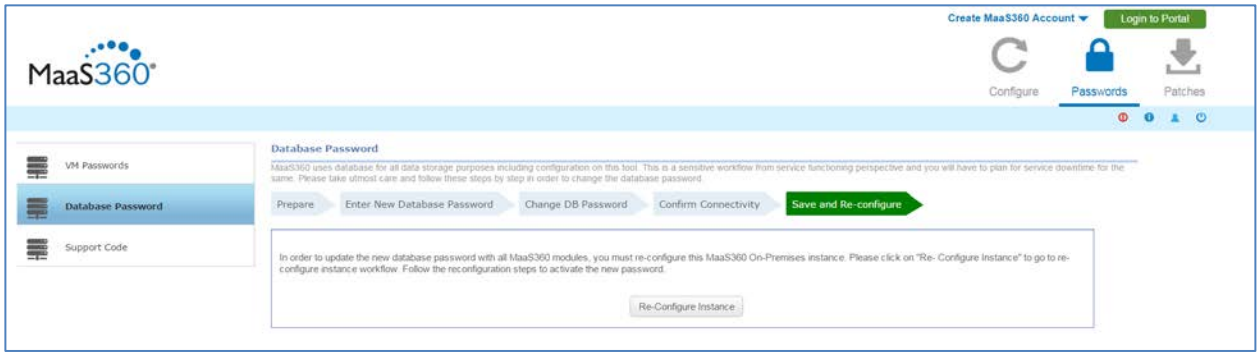
6. Confirm connectivity. A test will be done to verify the database connection for all VMs in the vApp. A green checkmark will indicate successful database connectivity test and a red X will indicate a failure. Ensure all VMs have green checkmarks, and then click **Save**.

   If there are any failures, click B**ack** to go back and make corrections.



7. Do not refresh the page while the Save process is underway.
8. The last step will apply the new database password to all the applications in the VMs, and will reconfigure them to start using this new password.

   Click **Re-Configure Instance**.



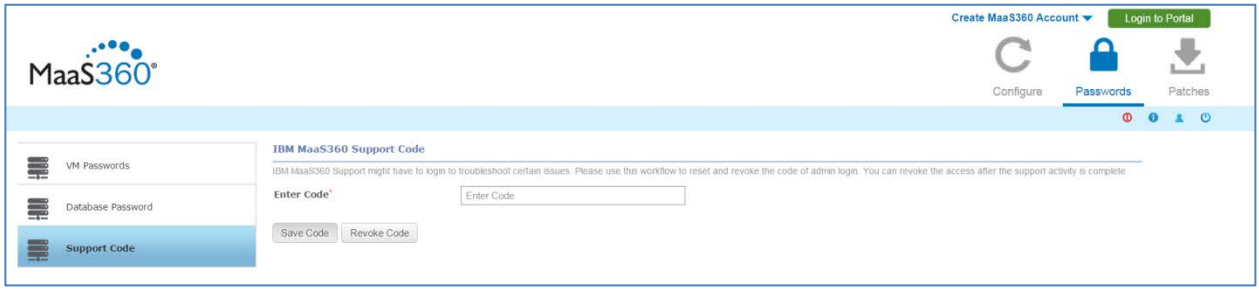
Support Code

It may become necessary for IBM Support to gain access to your deployment to troubleshoot issues.

The IBM MaaS360 Support Code workflow allows you to grant temporary remote access to your IBM MaaS360 environment to IBM support. This access can be granted for a support session and can be revoked once the support session is over.

To enable or disable a support code, perform the following steps:

1. From the Administration Console, access the **Passwords** tab in the upper-right corner of the UI and select **Support Code**.
2. Enter an access code provided by IBM Support in the **Enter Code** field.
3. Click **Save Code** to save and enable that access code. IBM Support can now access your IBM MaaS360 deployment.
4. After the need for remote access has passed, click **Revoke Code**. The entered code is no longer valid and IBM Support can no longer access your deployment.



Patches

Patches allow your IBM MaaS360 Mobile Device Management deployment to be modified between feature releases.

IBM can release security and functional fixes in the form of patches. Patches are applied using the **Patches** section of the Administration Console.

To patch your deployment, complete the following steps:

1. Click the **Patches** icon in the upper-right corner of the Administration Console.
2. Click **Upload New Patch** and navigate to the location where the patch is located.
3. Enter the checksum provided with the patch and click **Upload**.

The Next Step

With your database deployed, the IBM MaaS360 vApp deployed, and your deployment configured using the Administration Console, you are ready to begin using the Portal to customize your deployment in preparation for managing devices.

The next step is to create an IBM MaaS360 Mobile Device Management account, if you have not done so already. This process and further steps are described in the *IBM MaaS360 Mobile Device Management Configuration Guide*.

Appendix A: VM Internal Hostnames and IP Requirements

IBM MaaS360 is composed of seven virtual machines, which require their own static IP addresses.

The following IP entries are examples only. These examples should not be used, as is, for your environment.

Table 8. Virtual machine descriptions

Virtual Machine	Internal Hostname	Static IP	Description
Configuration VM	op1infra1-0.op1.sysint.local	Static IP 1	This VM is used for deployment and administration.
Portal VM	op1portalapp1-0.op1.sysint.local op1portalapp1-1.op1.sysint.local	Static IP 2 Static IP 5	These VMs host the portal, end user portal, and enrollment URLs. These VMs run several applications and are the primary console for IBM MaaS360 administrators. These VMs also host the Enrollment service that devices use to enroll as well as the End User Portal that is accessible by users to manage their own devices.
Services and CDN VM	op1svcapp1-0.op1.sysint.local op1svcapp1-1.op1.sysint.local	Static IP 3 Static IP 6	These are the VMs through which end user devices connect. These VMs act as a gateway for device communication and API calls. They also host the Content Delivery Network that delivers content to devices.
Standalone Batch Jobs VM	op1standalone1-0.op1.sysint.local op1standalone1-1.op1.sysint.local	Static IP 4 Static IP 7	These VMs run scheduled batch jobs.

Appendix B: Sample DNS Entries

Several DNS entries, Static IPs, and the natting between them must be set up.

IBM MaaS360 requires four DNS entries, one to four public IPs, and natting between the public IPs to the internal static IPs configured at the VM level.

The following DNS entries are examples only. These examples should not be used, as is, for your environment.

Note: *The example below is for single-instance deployment. You have to do the correct natting when using a load balancer or reverse proxy.*

Table 9. Sample DNS entries

DNS	Sample DNS	VM	Static IP	Natted Public IP	Description
Enrollments	mdm.company.com	Portal VM	Static IP 2	Public IP 1	Devices will enroll into IBM MaaS360 using this URL
Portal	mdmportal.company.com	Portal VM	Static IP 2	Public IP 1	This URL hosts the primary portal console for device administration.
Services	mdmservices.company.com	Services and CDN VM	Static IP 3	Public IP 2	This URL acts as a gateway for device communication and all communications after enrollments.
EUP	mdmeup.company.com	Portal VM	Static IP 2	Public IP 1	This URL is the End User Portal that is accessible by users to manage their own devices.

Appendix C: VM Root Log In

For security reasons, the root user cannot be accessed remotely. The user **maas** was created for remote access. After logging in as **maas**, you can elevate to root.

Execute the following commands for VM login as root:

```
ssh maas@op1infra1-0.op1.sysint.local

# The default password is MaaS360_Console

# To elevate to root user level

su

# The default password is MaaS360_Console

# Switch to the automation_prod user

su automation_prod
```

Note: *The internal hostname for the Configuration VM is an example.*

Appendix D: SSL Certificate Password Removal

You can use commands to generate an SSL key without a password from an SSL key containing a password.

Run the following commands:

```
#old.key is SSL key with password
#new.key is SSL key without password
openssl rsa –in old.key -out new.key
```